

Carl Westerlund

# Attityder till integritet på internet

Carl Westerlund

Åbo Akademi

Fakulteten för samhällsvetenskaper och ekonomi

Pro gradu, Statsvetenskap

Våren 2020

Ämne: Statsvetenskap	
Författare: Carl Westerlund	
Arbetets titel: Attityder till integritet på internet	
Handledare: Henrik Serup Christensen	
<p><b>Abstrakt:</b></p> <p>I undersökningen behandlas människors förhållningssätt till statlig övervakning online. Statlig övervakning online och de möjligheter människor har att upprätthålla sin integritet på internet är betydelsefulla för relationen mellan stat och individ. Dessa möjligheter har förändrats mycket de senaste tiotals åren. Graden av integritet på internet är en fråga om individens frihet i förhållande till staten, men även behovet av att begränsa sådan frihet. Undersökningens syfte är att utreda vilken attityd människor har till integritet på internet och vilka faktorer som påverkar deras attityd.</p> <p>I teoridelen av undersökningen presenteras olika perspektiv för att försöka förklara varför människor har den attityd de har, däribland överväganden gällande säkerhet och rätten till privatliv, institutionellt förtroende, politisk positionering och ekonomisk argumentation. Undersökningens analysdel använder data från två Pew Research enkäter som gjordes med syftet att utreda amerikaners attityd till integritet online, direkt efter Edward Snowdens publikation år 2013 av information gällande den amerikanska statens informationsinsamling. Dessa data används för att utföra en binär logistisk regressionsanalys med syftet att identifiera vilka faktorer som påverkar huruvida en person är orolig i förhållande till statlig informationsinsamling online, eller inte. Resultatet visar att graden av institutionellt förtroende har ett positivt samband till huruvida en person är orolig eller inte, medan hur mycket människor har hört om övervakning online med syfte att motverka terrorism, har ett negativt samband. Ålder uppvisade inget tydligt samband, trots att tidigare forskning funnit ett negativt samband mellan oro i förhållande till övervakning online och ålder.</p>	
Nyckelord: Integritet	
Datum: 27.02.2020	Sidoantal: 83

## Tabeller:

Tabell 1: Attityd till online-övervakning.....	s. 46
Tabell 2: Binär beroende variabel.....	s. 46
Tabell 3: Ålder.....	s. 50
Tabell 4: Kön.....	s. 50
Tabell 5: Politisk avvikelse.....	s. 51
Tabell 6: Tea Party.....	s. 51
Tabell 7: Institutionellt förtroende .....	s. 52
Tabell 8: Kännedom om övervakning med syfte att motverka terrorism.....	s. 52
Tabell 9: Utbildning.....	s. 53
Tabell 10: Bivariat, institutionellt förtroende.....	s. 61
Tabell 11: Bivariat, kännedom om övervakning med syfte att motverka terrorism...s.	61
Tabell 12: Bivariat, politisk avvikelse.....	s. 62
Tabell 13: Bivariat, Tea Party.....	s. 62
Tabell 14: Kodning för kategoriska variabler.....	s. 63
Tabell 15: Binär logistisk regressionsanalys resultat.....	s. 63
Tabell 16: Ordinal logistisk regressionsanalys resultat.....	s. 83
Tabell 17: Ordinal logistisk regressionsanalys resultat.....	s. 83

## Grafer:

Graf 1: Institutionellt förtroende.....	s. 66
Graf 2: Institutionellt förtroende.....	s. 66
Graf 3: Kännedom om övervakning med syfte att motverka terrorism.....	s. 67
Graf 4: Kännedom om övervakning med syfte att motverka terrorism.....	s. 67
Graf 5: Politisk avvikelse.....	s. 68
Graf 6: Politisk avvikelse.....	s. 69
Graf 7: Tea Party.....	s. 70
Graf 8: Tea Party.....	s. 70
Graf 9: Ålder, kategorisk.....	s. 71
Graf 10: Ålder, kategorisk.....	s. 71

	Innehållsförteckning	
1. Introduktion .....		5
1.1 Forskningsfråga .....		7
1.2 Disposition.....		7
2. Bakgrund .....		9
2.1 Begreppsdefinition .....		9
2.2 Historisk utveckling.....		10
2.2.1 Perioden 1945-1959.....		11
2.2.2 Perioden 1960-1979.....		11
2.2.3 Perioden 1980-1989.....		13
2.2.4 Perioden 1990-2002.....		13
3. Teori .....		16
3.1 Säkerhet vs. rätten till privatliv .....		16
3.2 Institutionellt förtroende och kollektivism .....		19
3.3 Kommersiella perspektiv .....		20
3.4 Integritetsnormer .....		23
3.5 Rationalitet .....		24
3.6 Tidigare forskning .....		25
3.7 Hypoteser.....		33
4. Forskningsdesign.....		37
4.1 Data .....		38
4.2 Urval.....		39
4.3 Operationalisering, validitet och reliabilitet .....		41
4.4 Beroende variabel .....		44
4.5 Oberoende variabler .....		47
4.6 Kausalitet.....		53
4.7 Generalisering.....		56
4.8 Statistisk Metod .....		57
5. Resultat .....		61
5.1 Bivariat analys .....		61
5.2 Binär logistisk regressionsanalys.....		62
5.3 Prediktiv sannolikhet för binär beroende variabel .....		64
6. Diskussion och konklusion.....		72
7. Avslutning .....		78
8. Källor:.....		80
9. Bilagor:.....		83

## 1. Introduktion

Under början av 1990-talet gjordes ett teknologiskt framsteg som förändrade världen, då skapades World wide web. Under några tiotals år blev denna uppfinning en allt mera integrerad del av i stort sätt alla delar av vårt samhälle: Det sätt vi kommunicerar på, vårt ekonomiska system, vår bokföring, hur vi uppfattar och deltar i politiken. Samtidigt som allt flera delar av samhället blev uppkopplade har även antalet användare ökat kraftigt. Utvecklingen under de senaste årtiondena har varit närmast explosionsartad. År 2000 fanns det 413 miljoner internetanvändare, år 2016 över 3.4 miljarder (Roser m.fl., 2019). En annan betydelsefull del av samhället som onekligen påverkats av denna utveckling är den gräns vi ofta drar, eller i alla fall försöker dra, mellan det privata och det offentliga. All den information som tidigare lagrades på papper i arkiv kunde, efter att datorer började användas av myndigheter och andra organisationer såsom företag under andra halvan av förra århundradet, lagras elektroniskt.

Efter att datorer för hemmabruk togs i bruk och internet fick sina första användare har det dock gradvis även varit andra former av data som kunnat samlas in om dessa användare. Ett exempel är data gällande vilka nätsidor någon besöker eller vilka e-mail någon skickar. Alla de metadata som beskriver vem som kommunicerar med vem, varifrån och inom vilket tidsintervall blev även tillgängliga för insamling. Denna informationsinsamling innebär naturligtvis en möjlighet för myndigheter och andra organisationer att övervaka vanliga privatpersoner. En fråga som verkar högst angelägen i dagens samhälle är därmed vilka konsekvenser insamlandet och användandet av all denna personliga information har för människors möjlighet att hålla det privata, privat. Mitt intresse, och ämnet för min avhandling, är hur människor förhåller sig till integritetsskydd på internet. Vilken syn har människor på att sådan informationsinsamling äger rum och vilka faktorer skulle kunna tänkas förklara deras förhållningssätt?

Många har kopplat ihop rätten till privatliv med demokrati. Att undvika omotiverad eller överdriven övervakning från statsmakten eller andra inflytelserika organisationer ses av vissa som en grundläggande demokratisk rättighet och någonting som skiljer

demokratier från diktaturer. Huruvida enskilda personers rätt till privatliv upprätthålls är en av de saker som reglerar förhållandet mellan stat och individ, och överdriven omotiverad övervakning är någonting som karakteriserar auktoritära samhällen. Vissa menar att människors möjligheter att ha verklig frihet, att vara kreativa, utforskande och tänka annorlunda är beroende av att de kan kontrollera vilken information om dem som andra, inklusive staten, känner till. Då du som medborgare inte vet när det du gör är privat och när det inte är det, eroderas den frihet som hör ihop med moderna demokratiska samhällen. Enligt ett sådant perspektiv borde även demos, d.v.s. folkets vilja och möjligheter att skydda sin rätt till privatliv vara av högsta intresse för statsvetenskaplig forskning.

Rätten till privatliv kanske är en del av demokrati, men säkerhet är även en del av ett fungerande samhälle och utan tillräcklig övervakning från statens sida är säkerhet inte möjligt. En av statens mest grundläggande uppdrag är att upprätthålla säkerhet. Terroristattentat och kriminella organisationers verksamhet möjliggörs av internet och staten kan höja invånarnas säkerhet och motverka brott genom online-övervakning. De som argumenterar för massövervakning av elektronisk kommunikation menar att de fördelar som kan nås med många, eller åtminstone en del av de program som organisationer som NSA (National Security Agency) i USA eller GCHQ (Government Communications Headquarters) i Storbritannien upprätthåller väger tyngre än potentiella nackdelar.

Oberoende av vilken position man har i förhållande till denna fråga, står det klart att de förutsättningar man har som individ för att upprätthålla ett privatliv och den kapacitet staten och andra organisationer har för att samla in personlig information om en, har förändrats radikalt under de senaste årtiondena. De faktorer som kan tänkas påverka möjligheterna till integritetsskydd kan enligt Alan F. Westin (2003, 2) delas in i tre kategorier. Dessa kategorier är: teknologi, socialt klimat och opinion samt organisationers policy och lagstiftning. Därutöver går det att skilja mellan tre olika sorters relationer som berörs av integritetsutvecklingen: mellan individ och stat/myndighet, mellan konsument och företag och mellan arbetstagare och arbetsgivare (Westin 2003, 2). Då vi diskuterar privatliv i ett statsvetenskapligt sammanhang är det väll framförallt den första av dessa relationer som är viktig, även om de två andra relationerna även är viktiga områden för lagstiftning och politisk debatt. Westin (2003, 6) skiljer mellan tre huvudkategorier av ideologisk position och intressebevakning

gällande integritet: “High-privacy”, “Limited-privacy” och “Balanced-privacy position”. “High-privacy position” innebär att integritet ses som det primära värdet. Andra värden blir därmed av lägre prioritet. “Limited-privacy position” ser integritet som mindre viktigt i förhållande till andra värden så som ekonomisk effektivitet och samhällets säkerhetsrelaterade övervakning. “Balanced-privacy position” är som namnet antyder en mellanform, där man vill undvika att rätten till privatliv utnyttjas oetiskt. En av de saker som Westin undersökte är hur andelen amerikaner som har en viss position i förhållande till integritetsskydd har förändrats över tid, samt vilka former av samhällsförändring som sammanfallit med denna positionsförändring.

## **1.1 Forskningsfråga**

I denna avhandling är jag alltså intresserad av att utreda vilken attityd människor har till integritet online, samt vilka faktorer som påverkar denna attityd. I teoridelen av min avhandling planerar jag att presentera olika teoretiska perspektiv som belyser denna fråga och tidigare forskning som har gjorts med liknande ändamål. I den empiriska delen av avhandlingen ämnar jag undersöka huruvida de hypoteser stämmer som jag kan formulera på basis av den teori jag behandlar. Min forskningsfråga är: Vilka faktorer förklara variationen i förhållningssätt till integritet online hos individer?

## **1.2 Disposition**

I följande kapitel, kapitel 2, behandlas hur begreppet integritet kan definieras och vilken betydelse detta begrepp får i min undersökning. Dessutom gör jag i avsnitt 2.2 en historisk genomgång av utvecklingen inom integritetsskyddsområdet under 1900-talets senare hälft. I kapitel 3 behandlar jag teoretiska perspektiv som kan tänkas förklara hur människor förhåller sig till integritet på internet. I avsnitt 3.1 behandlas rätten till privatliv vs. behovet av säkerhet, i 3.2 betydelsen av institutionellt förtroende och kollektivism, i 3.3 ser jag på kommersiella perspektiv på integritetsfrågan och i 3.4 behandlas integritetsnormer. Detta teoretiska underlag används för att avslutningsvis, i avsnitt 3.7, formulera hypoteser gällande svaret på min forskningsfråga, alltså vad som förklarar människors förhållningssätt till integritet på internet.

I kapitel 4 behandlas min forskningsdesign d.v.s. hur jag har gått till väga för att undersöka min forskningsfråga empiriskt. I detta kapitel presenterar jag mina olika variabler, hur jag mäter dessa, samt vilka problem som kan uppstå gällande sådant som validitet och reliabilitet. I detta kapitel behandlas även den statistiska metod jag använder mig av. I kapitel 5 presenteras resultatet av min statistiska analys och i kapitel 6 försöker jag avgöra hur detta resultat kan kopplas till mina hypoteser och teoretiska utgångsläge samt hur min forskningsfråga skall besvaras. Kapitel 7 är avhandlingens avslutande kapitel och behandlar betydelsen av integritet i dagens samhälle och sammanfattar resultatet av min undersökning.



## 2. Bakgrund

### 2.1 Begreppsdefinition

I min avhandling utgår jag ifrån det engelska begreppet "privacy". Detta begrepp motsvaras på svenska av begrepp såsom integritet, privatliv, hemlighållande eller avskild. Som begrepp kan det definieras t.ex. som människors anspråk på att få bestämma över vilken information om dem som andra har tillgång till. Det involverar även när sådan information kommer till andras kännedom och hur den används (Westin 2003, 3). Jag kommer att använda de svenska orden integritet och privatliv, men även beroende av sammanhanget tala om "integritetsskydd" eller "skydd av privatliv".

"we define privacy as the degree to which personal information is not known by others"(Kannan m.fl. 2002, 3). Enligt denna definition minskar en individs nivå av integritetsskydd desto mera andra, så som myndigheter, känner till om denna.

Ferdinand D. Schoeman (1992, 13) menar att integritet, och de normer som skapar förutsättningar för integritet, kan delas in i två kategorier. Den första formen av integritet handlar om att undanhålla sådana delar av ens liv från andra som skulle kunna påverka ens värdighet på ett negativt sätt. Den andra formen av integritet handlar om skyddande av ens möjligheter att uttrycka sig och om att motverka social kontroll (Schoeman 1992, 14). Enligt ett sådant perspektiv handlar integritet inte enbart om att kontrollera vad andra känner till om en själv, utan även om att vara fri i sin sociala interaktion. Detta skulle säkert många koppla ihop med autonomi eller yttrandefrihet snarare än integritet.

Ett sätt att definiera det privata är naturligtvis i förhållande till det offentliga. Zizi A. Papacharissi (2010, 27) anger två sätt att komma åt denna distinktion: "(a) What is hidden or withdrawn versus what is open, revealed, or accessible; or (b) what is individual, or pertains only to an individual, versus what is collective or affects the interest of a collectivity of individuals."

Ovanstående definitioner handlar om integritet i allmänhet. Dock verkar det som om vad man menar i ett online-sammanhang, då man talar om integritet online, inte skiljer sig väsentligt från mera allmänna begreppsliga innebörder. Vad jag avser med integritet i denna avhandling är undanhållandet av sådan information från andra, som handlar om oss själva som individer, d.v.s. personlig information. Med personlig information avser jag alltså sådan information som på något sätt handlar om en individ eller kan ge någon insikter om denna person genom härledning. Det kan vara fråga om vilka intressen någon har, vad någon är intresserad av att köpa, medicinska data, politiska kopplingar etc. Vissa delar av denna information beskriver vad någon gör på online, andra delar är härledda från denna information t.ex. vad någon är intresserad av att köpa. I ett online sammanhang kan det t.ex. handla om data man själv laddar upp eller data någon annan laddar upp gällande en, samt data gällande vem man kommunicerar med eller vilken information man söker upp.

Det jag mera specifikt skall försöka utreda är alltså den attityd människor har till att personlig information som genereras då de använder internet eller laddas upp, samlas in av organisationer, först och främst av myndigheter. Ett exempel på sådan insamling är massinsamling av e-mail metadata av NSA och vilken attityd amerikaner har i förhållande till detta. Då mera sådan data samlas in, minskar följaktligen den information om oss som vi har möjlighet att undanhålla och därmed minskar vår integritet. Till näst skall jag behandla den historiska utvecklingen inom detta område, vilket har syftet att förklara varför vi nått den situation vi befinner oss i och hur den allmänna opinionen har utvecklats.

## 2.2 Historisk utveckling

Under de senaste ca 70 åren har det skett en hel del utveckling på integritetsområde, vilket inte enbart handlat om teknologisk utveckling. Den allmänna opinionen om ämnet har gradvis förändrats och mycket lagstiftningsarbete har utförts. Inledningsvis ämnar jag ge en översiktlig beskrivning av denna historiska utveckling för att sedan fokusera vid de senaste årtiondena av utveckling. Under denna senare tid har människor varit aktiva internetanvändare och mitt mål är att försöka hitta en teoretisk bakgrund till

hur människor i dagens läge kan tänkas förhålla sig till integritetsskydd inom ett online-sammanhang.

Alan F. Westin redogör i *Social and Political Dimensions of Privacy* för tre faser av utveckling inom integritetsskydd som samhällsfenomen med en grundperiod som utgångsläge. Grundperioden är 1945-1959 och de tre faserna är 1945-1959, 1961-1979, 1980-1989 och 1990-2002. Därefter ser han på vilken innebörd terroristattentatet 11.9.2001 hade för integritet. Denna undersökning handlar nästan uteslutande om USA men mycket kan även kopplas till utvecklingen i andra delar av världen, t.ex. Europa.

### **2.2.1 Perioden 1945-1959**

Utgångsläget för hans historiska genomgång är som sagt perioden 1945-1959. Denna period karakteriserades av begränsade möjligheter för övervakning samt ett högt institutionellt förtroende hos den amerikanska befolkningen. Bakgrunden till denna situation är andra världskrigets slut och att kommunister och sovjetunionen var en extern hotbild (J.B. Rule, 2009). Därutöver hade "civil-rights" rörelsen inte ännu kommit igång och institutionell diskriminering var ännu vanligt. (Westin 2003, 6)

Inom lagstiftning gjordes några första steg mot att trygga människors rätt till privatliv. Det var mot bakgrunden av sådana intrång i människors privatliv som fascistiska regimer gjort sig skyldiga till, som Förenta Nationerna år 1948 inkluderade rätten till privatliv som en mänsklig rättighet i den allmänna förklaringen om de mänskliga rättigheterna (Jan Holvast 2009, 29). År 1950 tillkom "the European Convention for the Protection of Human Rights and Fundamental Freedoms. Artikel 8 anger att: "Everyone has the right to respect for his private and family life, his home and his correspondence". Det nämns dock även vissa undantag till denna rättighet, bland annat vid behov relaterade till nationell säkerhet (Jan Holvast 2009, 29).

### **2.2.2 Perioden 1960-1979**

Den första eran, för Westin, efter denna grundperiod är perioden 1960-1979. Under denna tidsperiod inträffade några viktiga teknologiska framsteg inom automatisering, vilket fick konsekvenser för sådant som upprätthållandet av databaser. Det fanns dock redan i ett tidigt skede personer som såg automatisering som någonting riskfyllt och

den kritik som framfördes drev även amerikanska myndigheter till att utreda integritetsrelaterad oro och behovet av lagstiftning (Westin 2003, 9-11).

I Europa fanns det även liknande initiativ. Under slutet av 1960-talet beslöt sig Europarådet för att utreda hur väl skyddade individuella rättigheter var, givet den tekniska utveckling som skett inom informationsteknologi och användning av personliga data, genom att utföra en enkätundersökning. Undersökningen kom till slutsatsen att det inte fanns tillräckligt skydd och år 1976 skapades "Committee of Experts on Data Protection", som i sina slutsatser, som publicerades år 1979, lade grunden för "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data" (Stratford & Stratford 1998, 19). Denna konvention skapade bl.a. principer för integritetsskydd för data och principer för dataflöden. Antagandet av konventionen skedde år 1995, vilket innebar att medlemsländerna skulle börja anpassa sin lagstiftning efter konventionens ändamål (Stratford & Stratford 1998, 19).

På den politiska arenan inträffade även ett antal viktiga händelser som förändrade de amerikanska väljarnas syn på dataskydd och påverkade nivån av institutionellt förtroende. Politiska skandaler beträffande Nixon-administrationen, samt CIA:s och FBI:s maktövertramp ledde till mindre förtroende för offentliga institutioner (J.B. Rule, 2009). Journalister spelade en viktig roll för att avslöja myndighetsövertramp men bidrog även själva till att människors rätt till privatliv kränktes. Detta riktade in sig mot kända personer med målet att göra ekonomiska vinster (Westin 2003, 11).

Det gjordes framsteg för att trygga människors grundläggande rättigheter då det under denna tid togs initiativ för att avsluta institutionell diskriminering. Man genomdrev även en del ny lagstiftning för skyddandet av rätten till privatliv: "federal privacy act of 1974" och "Educational Rights and Privacy Act" (1974) och "the Right to Financial Privacy Act" (1978). Politiskt sett var man inte nödvändigtvis uppdelade längs en traditionell höger-vänster skala, utan libertinister, konservativa och liberala var ofta på samma sida gällande integritet-policy (Westin, 2003, 8).

Under denna tid gjorde man en del socialvetenskaplig forskning för att undersöka amerikaners syn på integritet t.ex. *The Dimensions of Privacy*, 1978. Det var den första studien av sitt slag som såg på den amerikanska befolkningens attityd till integritetsskydd. Man fann bl.a. att amerikaner upplevde att deras nivå av integritet i

förhållande till människor i deras näromgivning, så som grannar, var på en hög nivå. 76 % ansåg att rätten till privatliv borde inkluderas i “the bill of rights”(den amerikanska rättighetsförklaringen) och det fanns ett klart stöd för lagstiftning för att garantera denna rättighet mellan individer och olika institutioner. Sambandet mellan förtroende för samhällets olika institutioner och hur oroliga respondenterna var för integritetskränkningar analyserades även, vilket uppvisade ett positivt samband (Westin 2003, 12).

### **2.2.3 Perioden 1980-1989**

Följande era som Westin behandlar är från 1980 till 1989. Denna period innehöll en del viktiga framsteg inom informationsteknologi såsom att “distributed computing” började användas vid upprätthållande av data samlingar samt “Workplace video display terminals” (VDTs) och PC:n. Det genomfördes även ny lagstiftning till stöd för integritetsskydd och för att begränsa övervakning på arbetsplatsen, såsom “the Cable Communications Policy Act of 1984”, som krävde att kabel-företag skulle informera sina kunder om sin datainsamling och ge dem rätt till de insamlade data (Westin 2003, 15). Dock var dataskyddslagstiftning i USA, till skillnad från i Europa, i första hand sektor baserad och inriktad på förhållandet mellan stat och individ (Stratford & Stratford, 1998; Westin 2003, 16).

Politiskt sätt var integritetsskydd fortsättningsvis en fråga för både högern och vänstern. För högern främst gällande statlig övervakning. Under denna period gjordes ytterligare forskning beträffande den amerikanska allmänhetens attityder till integritetsskydd, så som: the road to 1984 av Harris år 1984. Han undersökte allmän opinion i förhållande till ny informationsteknologi. Vad han kunde se var att allmänheten var tudelad. Människor uppskattade fördelar och bekvämlighet, men var oroliga över potentiell felanvändning (Westin 2003, 14).

### **2.2.4 Perioden 1990-2002**

I allmänna drag handlade dessa två inledande perioder om hur teknologisk förändring under andra halvan av förra århundradet skapade nya möjligheter för övervakning och datainsamling om privatpersoner av stat och företag. Förtroende för offentliga institutioner och deras övervakning gick neråt då de risker som existerade blev allt

tydligare för allmänheten och det uppstod skandaler kring myndighetsövertramp. Dessutom genomdrevs ny lagstiftning för att trygga rätten till privatliv. Integritetsskydd var dock inte ännu ett “first-level issue” i USA. Det blev det dock under den 3: dje perioden mellan 1990 och 2002 (Westin 2003, 17). Då inträffade fem viktiga teknologisk förändringar: www, Mobile communication devices, Human genome project, Datamining och Statliga försök att förhindra privata aktörer från användandet av enkrypteringsverktyg samt utvecklandet av FBI:s “carnivore program” med syftet att övervaka kommunikation online. Man var orolig att sådana “verktyg” skulle användas av kriminella ss. terrorister och drogförsäljare (Westin 2003, 17).

“We must know you to serve you” kan anses vara 1990-talets modell för hur företag förhöll sig till konsumenter. Att företag kände till var människor befann sig vid vilken tidpunkt, är ett exempel på en effekt av den teknologisk förändring som ägde rum under denna period. De strategier företag kunde börja använda sig av väckte irritation hos konsumenter och presenterades i media som “privacy-intrusive business marketing”. Genom allt större internetanvändning och t.ex. användningen av kreditkort, kunde man börja samla in allt mera information om privatpersoners beteende (Westin 2003, 18). Att använda sig av medicinska data och genetiska data för att t.ex. avgöra möjligheten till hälsovårdsförsäkring, sågs av förespråkare för rätten till privatliv som ett stort problem. Ekonomiska brott så som identitetsstöld och stöld av data från offentliga arkiv gick upp, vilket ledde till oro beträffande datasäkerhet. De risker som den teknologiska utvecklingen skapade var allt tydligare.

EU försökte skapa möjligheter för informationsflöde mellan sina 15 (år 1990) medlemsländer och försökte reglera dataflödet för att upprätthålla dataskydd, t.ex. genom “EU Data Protection Directive” år 1995. Stora företags möjligheter att skicka data om anställda och konsumenter från EU till sina ursprungsländer begränsades, med villkoret att dessa länder skulle leva upp till EU:s standarder gällande dataskydd (Westin 2003, 19). I regel var företag ovilliga att acceptera omfattande privatskydd för konsumenter, med en del undantag. Samtidigt uppstod det allt flera intressegrupper för att understöda ökat integritetsskydd. Undersökningar som gjordes mellan 1990-1995 visar en trend, där allmänhetens oro är på klar uppgång gällande integritetsskydd i förhållande till myndigheter och företag: “Respondent concern about threats to their personal privacy jumped from 64 % in 1978 to 84 % in 1995” (Westin 2003, 21). Det här sammanhänge med en nedgång i institutionellt förtroende (Westin 2003, 21).

Företagens informationsinsamling sågs som ett allt klarare hot mot integritetsskydd: “80% agreed by 1995 with the statement that consumers have lost all control over how companies collect and use consumer personal information” (Westin 2003, 21). Ett kontrast till den minskade tilltron till institutioner och oron över datainsamling var hur arbetstagare hade blivit mera positivt inställda till övervakning på arbetsplatsen under slutet av 90-talet. Vilken slags relation och social miljö det är frågan om, påverkade alltså inställningen till integritetsskydd.

År 1995 gjordes en Harris-Westin enkätundersökning som visade vilken uppdelning allmänheten hade gällande integritet: 25 % high-privacy/ privacy fundamentalists, 20 % privacy-unconcerned, 55 % balanced/pragmatists. 1996-1999 gjordes en andra omgång. Då visade det sig bl.a. att internet förorsakade allt mera oro beträffande integritetsskydd. Andelen människor som sade sig vara oroliga att information felanvändes steg. Samtidigt såg många personer fördelar med att företag samlade in information som kunde förbättra deras service. Man hade fortfarande förtroende för att företag behandlade konsumenters personliga information på ett ansvarsfyllt sätt. Detta hade förändrats dramatiskt i de Harris-Westin undersökning som gjordes 2001-2002: Nu uppfattade allmänheten att företag inte gick att lita på gällande integritetsskydd och att lagar för att säkerställa konsumenters integritetsskydd inte var tillräckliga. Andelen människor som kunde kategoriseras som “privacy-unconcerned” sjönk till 8 %. Det fanns 3 orsaker till denna förändring i allmän opinion: 1) Sammanslagning av banker, försäkringsbolag och investeringsbolag med den amerikanska kongressens tillåtelse. Det innebar att personlig data som tidigare varit separat inom olika sektorer nu kunde sammanföras, t.ex. hälso- och finansinformation (Westin 2003, 21).

2) The federal Health Insurance Portability and Accountability Act of 1996. Denna lag gav hälsosektorn målet att de skulle göra sina datasystem elektroniska, d.v.s. alla hälso- och administrativa uppgifter skulle börja sparas och bearbetas elektroniskt (Westin 2003, 21). 3) Internetanvändares oro över deras data blev allt större, vilket påverkade deras attityd till integritetsskydd (Westin 2003, 21). Denna förändring gav upphov till att stora mängder lagstiftning, med målet att skapa ett starkare integritetsskydd, genomdrevs under början av 00-talet, trots företags motvilja. Politiskt sätt uppstod en koalition kring integritetsfrågan mellan liberala, konservativa och libertinister. Den sistnämnda gruppen var dock mera intresserad av marknadslösningar, medan de två tidigare förespråkade statlig reglering (Westin 2003, 26). Den tredje perioden

avslutades av händelserna den 11 september 2001 och de konsekvenser detta terroristattentat fick för allmän opinion i förhållande till integritetsfrågan och de amerikanska myndigheternas övervakning.

### **3. Teori**

I detta kapitel skall jag gå igenom olika teoretiska perspektiv som kan tänkas förklara varför människor relaterar till integritet online på det sätt de gör. Människors förhållningssätt är dels beroende av deras kännedom om huruvida och i vilken mån integritet är möjligt, dels deras principer och de preferenser de har. Sociala normer är även betydelsefullt. Till att börja med skall jag behandla balansen mellan integritetsskydd och säkerhet ur ett amerikanskt perspektiv.

#### **3.1 Säkerhet vs. rätten till privatliv**

Då man utreder integritet på ett ideologiskt plan eller försöker förstå varför myndigheter handlar som de gör, framstår ett klart mönster kring motiveringarna för och emot insamlandet av personliga data. De överväganden som ligger till grund för hur människor ser på denna fråga och hur institutioner motiverar sitt agerande kan grovt delas in i argument gällande behovet av övervakning för att uppnå säkerhet och behovet av att skydda människors rätt till privatliv (Bakir m.fl. 2015, 7). I USA har vissa händelser fått allmänheten att uttrycka en större acceptans för att statsmakten gör intrång i deras privatliv efter att externa hot, såsom terroristattacken 11.9.2001, skapade en efterfrågan på säkerhet.

Då det finns en sådan efterfrågan uppstår det lätt en debatt där privatliv och säkerhet ses som motsägelsefulla i förhållande till varandra. För att staten skall kunna garantera medborgares säkerhet i förhållande till externa hot, måste en del av medborgarnas integritet offras. Ett problem som kan tänkas uppstå i valet mellan säkerhet och integritet, är enligt viss observatörer att allmänheten inte har tillräckligt goda insikter i hur de olika strategier som myndigheterna använder sig av fungerar, då övervakning som policy-område kan vara för komplicerat för "vanliga människor" att förstå (Potoglou m.fl. 2017, 2).



Efter terroristattacken i USA 11.9.2001 har det genomförts flera statliga beslut och lagstiftning som ökat övervakningen av bl.a. amerikanska medborgare, t.ex. the Patriot Act of 2001, the Homeland Security Act of 2002 (Dinev m.fl., 2008; Evans, 2002). Ett annat exempel är Storbritanniens Draft Investigatory Powers Bill, som innebär att vanliga internetanvändares webbläsar-historik sparas så att den är lätt att använda av myndigheterna ifall undantagstillstånd (s.k. state of emergency) deklarerats (Potoglou m.fl. 2017, 2). Den här sortens politiska beslut har på många håll skapat en kontroversiell debatt som å ena sidan handlat om integritetsskydd och kritik av statens kränkande av medborgares rättigheter, å andra sidan om behovet av säkerhet vid hotet av terrorism och annan brottslighet. Då händelser som hotar säkerheten, t.ex. Terroristattentat, inträffar, höjs allmänhetens acceptans för övervakning. Denna acceptans sjunker sedan på nytt när man återgår från krisläge till "business as usual" och de risker som övervakning innebär återfår uppmärksamhet (Dinev m.fl. 2008). Detta beteende kunde man se året efter terrorattacken 11.9.2001. Direkt efter attentatet var den amerikanska allmänhetens acceptans av ökade befogenheter för myndigheterna, t.ex. gällande övervakning, på en hög nivå och det allmänna förtroendet för staten var högt. Efter kring ett år hade dock läget normaliserats och den offentliga diskussionen började allt mera kretsa kring de negativa sidorna hos övervakning och myndigheternas maktmissbruk (Dinev m.fl. 2008). Terroristattentatet den 9:e september 2001 skapade en chock och känsla av kris som hade en tydlig inverkan på amerikanska medborgares attityd till övervakning. I enkätundersökningar som gjordes efteråt kunde man se att amerikaner i allmänhet understödde flera olika former av övervakning. Det allmänna förtroendet för statsmakten ökade, från kring 30 % sommaren 2001 före terroristattentatet till nästan 60 % efteråt (Westin 2003, 28).

Man såg dock dessa former av övervakning främst som ett nödvändigt ont. Det fanns från första början en oro över potentiella statliga maktövertramp. Understödet för denna statliga övervakning med syfte att motverka terrorism var fortfarande högt, om än något lägre, under början av 2002, medan förtroende för statsmakten hade sjunkit till 40 %. Antalet personer med starkt förtroende för att staten inte kommer att använda sina nya maktbefogenheter på ett oetiskt sätt hade även sjunkit från 34 % till 12 % (Westin 2003, 28). De två främsta faktorerna som verkar ha påverkat dessa attitydförändringar var förekomsten/avsaknaden av flera framgångsrika terroristattacker, samt allmänhetens uppfattning om hur väl myndigheterna hade hållit sig inom gränserna för syftet med

sina utökade övervakningsbefogenheter eller hur många fall av maktmissbruk som skett med hjälp av dem. Det ökade förtroendet för myndigheterna och allmänhetens stöd för övervakning reflekterades inte i förtroendet för företag eller i en minskad oro över integritetsskydd i relationen mellan konsumenter och företag (Westin 2003, 29).

Amerikaner sätter, enligt undersökningar som gjorts under de senaste årtiondena, ett högt värde vid integritetsskydd. Man har upptäckt ett cykliskt mönster i hur mycket allmänheten bryr sig om integritetsskydd i USA. Dessa cykler är ca 10 år långa perioder som inleds av en "erosion" av integritetsskydd t.ex. som en konsekvens av nya teknologiska möjligheter till övervakning. Det leder till att oro gällande integritetsskydd lyfts upp på den politiska agendan. Sedan avtar graden av uppmärksamhet på detta område på nytt innan nästa liknande "erosion" inträffar (Dinev m.fl. 2008). Det verkar sannolikt att värdet människor ger övervakning för att nå mera säkerhet även kan variera på ett liknande sätt.

En annan observation som gjorts gällande utvecklingen inom integritetsskyddsområdet är att gränsen mellan statliga hot mot integritetsskydd och den privata sektorns motsvarande hot, har suddats ut. Även om det kanske verkar som om dessa två hot är två olika frågor, är dessa aktörer i praktiken ofta kopplade till varandra. Man kan tala om ett "surveillance-industrial complex" (Zavrsnik m.fl., 2015), där staten och företag samarbetar och staten får information om internetanvändare av de företag som samlat in informationen för kommersiellt bruk. Cyber-Security Enhancement Act (CSEA) of 2002: "sanction the exchange of certain information collected in the private sector with the agencies in the public sector" (Dinev m.fl. 2008, 216). Då man diskuterar integritetsskydd går det därmed inte alltid att hålla isär de fall som relaterar till myndigheter och de som relaterar till den privata sektorn.

En teoretisk anledning till att internetanvändare kan tänkas acceptera informationsinsamling om dem, eller rent av understöda sådan insamling, är alltså ett upplevt behov av övervakning. Det hänger samman med upplevda risker som behöver hållas under kontroll av de institutioner som genomför övervakningen. Denna motivering är även giltig i ett online sammanhang: "Over the Internet, risk can come from two sources: unauthorized access to digitized information and threats to the infrastructure" (Dinev m.fl. 2008, 220). För att man skall kunna skydda sig mot olika cyberbrott som att t.ex. bli lurad på pengar, behövs ur detta perspektiv övervakning på

internet. Det uppstår en situation där man måste ge staten tillgång till personlig information för att säkerställa att en tredje part inte olovligt får sådan tillgång. Det handlar alltså om ett slags kompromiss. Man kan välja mera integritetsskydd eller mera övervakning, där mera övervakning potentiellt leder till mera effektiv brottsbekämpning och högre säkerhet i samhället samt, paradoxalt nog, bättre integritetsskydd.

### 3.2 Institutionellt förtroende och kollektivism

Då man diskuterar integritet, är det förtroende människor har för myndigheterna en faktor som vissa har framfört som en möjlig förklarande variabel. Huruvida man litar på myndigheterna och andra informations- insamlade aktörer eller inte, kan tänkas påverka vilka val man gör gällande integritet. Studien *Internet Users' Privacy Concerns and Attitudes towards Government Surveillance – An Exploratory Study of CrossCultural Differences between Italy and the United State* (Massimo m.fl. 2005) ser på skillnader mellan amerikanska och italienska medborgares villighet att lämna över personlig information vid online transaktioner (e-Commerce), samt skillnader mellan dessa två grupper gällande deras attityd till statlig övervakning. Dessutom försöker man hitta bakgrundsfaktorer som kan tänkas förklara dessa skillnader. Skillnaden i förtroende för myndigheter mellan människor i dessa två länder är en faktor som påstås kunna förklara skillnaden i hur stort behovet av övervakning anses vara i respektive land.

En annan möjlig förklaring som lyfts fram i denna undersökning är graden av kollektivism. Denna faktor anses främst påverka vilken attityd människor har till rätten till privatliv. I den teoretiska delen av undersökningen framställer man argumentet, att samhällen som är mera kollektivistiska, t.ex. har en starkt familjecentrerad kultur, inte understöder individuella rättigheter så som rätten till privatliv i lika stor utsträckning. Integritet som politiskt värde är alltså starkt sammankopplat med individualism, enligt detta perspektiv. Andra undersökningar har även indikerat en liknande koppling (Li m.fl. 2017). Man tar därmed ett teoretiskt perspektiv som även tar sociala normer på ett större allvar. Att tänka sig att individen fattar rationella val på basis av för och nackdelar hos olika alternativ, t.ex. gällande mera eller mindre övervakning, är inte ett antagande man nödvändigtvis måste göra. Detta perspektiv skall jag gå närmare in på längre fram i detta kapitel (s. 21).

Övervakning har av vissa teoretiker ansetts vara kopplat till modernism. I enlighet med ett modernistiskt perspektiv försöker statsmakten ha allt större kontroll över vanliga människors liv. Det finns med andra ord de som ifrågasätter den officiella motivering som mera övervakning ges av myndigheter och förespråkare för mera övervakning. "Surveillance refers to any collection and processing of personal data, whether identifiable or not, for purposes of influencing or managing those whose data have been garnered" (Lyon 2001 refererad i Dinev m.fl. 2002). Ur ett sådant perspektiv ses alltså den övervakning som myndigheter och andra organisationer utför, huvudsakligen som någonting illegitimt. Det verkar sannolikt, på basis av ett sådant synsätt, att människor har en rätt så negativ attityd i förhållande till informationsinsamling och ett lågt förtroende. Dock förutsätter det att människor är medvetna om statens försök att kontrollera dem. Om man tror att statens främsta anledning till att övervaka, t.ex. Att samla in personlig data online, är att kontrollera människor, leder det således till att man knappast är intresserad av att offra sin integritet med löftet om högre säkerhet och mindre risk för att bli ett cyberbrottsoffer.

### **3.3 Kommersiella perspektiv**

Ett annat sätt att argumentera gällande graden av integritet är från ett kommersiellt perspektiv. Då företag har tillgång till mera data om sin kunder, kan de tjänster och produkter de erbjuder, bättre anpassas till konsumenternas behov och reklamförning kan göras mera effektiv (Kannan m.fl. 2002). Denna retorik är även vanlig då företag motiverar sin datainsamling. Kostnaden för att få information om konsumenter d.v.s. insamlandet, sparandet och analysen av data, har blivit allt lägre p.g.a. framsteg inom informationsteknologi, först och främst övergången till online-transaktioner (Movius m.fl. 2009). Att internetanvändare själv ofta fyller in information om sig själva vid online-interaktion med företag för att möjliggöra olika transaktioner, gör även insamlandet billigare. Att ha tillgång till sådan information är ekonomiskt lönsamt för företag då det hjälper företag att skapa tjänster och reklam som är bättre anpassad till enskilda konsumenter. Samtidigt som kostnaderna har gått ner har värdet sådan information har för företag gått upp då en sådan personifiering av t.ex. Reklam, blivit en allt mera dominerande strategi (Kannan m.fl. 2002; J.F. Rayport m.fl. 1997).

Då myndigheterna blivit allt mera angelägna om att övervaka med motiveringar så som terrorism- och cyberbrottsbekämpning, har det även uppstått en viss allmän efterfrågan

efter s.k. "Privacy Enhancing Technologies" eller PET:s. Dessa verktyg ger internetanvändare möjlighet att på olika sätt försöka bevara sin integritet, t.ex. Genom att hålla dem anonyma eller effektiv kryptering av online-kommunikation (Potoglou m.fl. 2017, 2).

I undersökningen *Customer economics of internet privacy* presenterar Kannan m.fl. 6 stycken antaganden som kan göras gällande förhållandet mellan teknologi, online-ekonomi och privatliv. Det första antagandet är att teknologi utvecklas över tid. I modern tid, med snabb teknologisk utveckling, är det knappast någon som tvivlar på detta antagande. En konsekvens av denna utveckling, kan antas vara, att kostnaden för att skaffa och processera personlig information går ner, vilket är det andra antagandet. Det har naturligtvis en betydelse för företags vilja att ägna sig åt sådan informationsinsamling vilket i sin tur påverkar deras beteende, vilket påverkar den allmänna opinionen gällande integritet online. Det tredje antagandet är att det ur konsumenters synvinkel finns en ideal nivå av integritet, där för lite integritet inte är önskvärt samtidigt som för mycket integritet även är det på grund av ensamhet. Människor kan uppleva ett behov av att vara ensamma lika väl som ett behov av kommunikation, gemenskap och att dela med sig till andra.(Westin 2003, 5).

Vad jag tänker att man menar med ensamhet (eng: loneliness) i detta sammanhang, är social isolering. Att bli övervakad av staten kanske inte gör någon mindre socialt isolerad, men kanske man kan tänka sig att det påverkar vilken attityd man har till integritetsskydd generellt sätt? De tre sista antagandena relaterar till hur integritet kan vara en produkt eller tjänst som alltså kan säljas. De första två av dessa antaganden är att integritet kan säljas som enheter av integritet, för ett visst pris per enhet och att varje enhet som säljs är information som företag inte har om den konsument som köper den. Det sista antagandet är att den personliga information som hålls privat för ett visst pris, enbart är sådan information som har ett högre värde för företag än kostnaden av att skaffa ifrågavarande information.

Dessa antaganden beskriver hur människors attityd till integritet även påverkas av vissa ekonomiska faktorer. Då integritet är en produkt som kan köpas blir samtidigt avsaknaden av integritet möjligtvis en produkt som vanliga människor kan sälja till företag (J.F. Rayport m.fl. 1997). Den här sortens ekonomiska argument påverkar säkerligen även människors attityd till upprätthållande av integritetsskydd. Man skulle

kunna fråga sig om det kommer att leda till att integritetsskydd i framtiden kan bli en lyx. Redan i dagens läge finns det skillnader mellan nivån av integritet för olika grupper i samhället, t.ex. mellan dem som söker sociala förmåner och därför måste lämna ut viss information och dem som inte gör det (Westin 2003, 4).

Om integritetsskydd blir en tjänst som konsumenter kan köpa av företag eller något som kan säljas, försätter det personer med olika stora ekonomiska tillgångar i en ojämlik position. Var man bor kan även ha betydelse för vilka förutsättningar man har i förhållande till övervakning. Tätbefolkad stadsmiljö och glesbefolkad landsbygd är till exempel olika i det här avseendet. Hur höga inkomster man har kan alltså vara avgörande för vilken attityd man har till integritet eftersom högre inkomster innebär att man har råd med integritetsskydd. Varför inte låta företag och myndigheter samla in all den information de vill ifall du kan köpa det alla andra förlorar? Detta förutsätter förstås att priset är tillräckligt högt för att ha en klar betydelse.

En av konsekvenserna av storskalig informationsinsamling av företag och myndigheter är vad man kallar ett asymmetrisk informationsförhållande. Detta innebär en situation där vissa aktörer har mera eller bättre information än andra. Vissa teoretiker menar att då det blivit allt lättare att få tag på personlig information om privatpersoner, d.v.s. då anskaffningskostnaderna för att få sådan information har gått ner, har detta skapat en situation där myndigheter och stora företag lätt kan samla in sådan information. Detta har skapat ett asymmetriskt informationsförhållande mellan privatpersoner och dessa aktörer (Dinev m.fl. 2008, 217).

Dessutom har många konsumenter bristfällig kunskap om vem som får tillgång till deras personliga information och till vilka syften den används. Det ökar asymmetrin i informationsförhållandet. Denna asymmetri gör eventuellt konsumenter mindre benägna att dela med sig av personlig information vid ekonomiska transaktioner som kräver sådan informationsdelning (Dinev m.fl. 2008, 218). Det verkar sannolikt att utelämnande av personlig information till statsmakten följer ett liknande mönster. Då man som medborgare har dålig insikt i vad myndigheter gör med ens information och ett asymmetriskt informationsförhållande har uppstått kan detta säkert tänkas göra en mindre välvilligt inställd till att lämna över ytterligare personliga data. Att vara negativt inställd till övervakning kanske inte nödvändigtvis grundar sig på de negativa

konsekvenser du tror övervakning innebär, utan på osäkerhet gällande vilka konsekvenserna kommer att vara.

Internet och användning av datorer har i många avseenden gjort det svårare att sträva efter integritet. Datorer var ursprungligen inte väl designade för att upprätthålla användarens integritet och internet har gjort många sammanhang som tidigare kunde antas vara privata till en del av det offentliga. En framtid utan några sammanhang, platser eller situationer, där man inte vet om man är övervakad, ses av vissa som en realistisk möjlighet (Kannan m.fl. 2002). Det är dessutom väldigt vanligt att internet-sidor inte enbart samlar in information om dem som besöker sidan utan även delar denna information med någon tredje part. Detta informationsdelande, ofta informationsförsäljande, ger privatpersoner ännu mindre kontroll över sin integritet online. Pessimistiska observatörer menar att integritet på internet, p.g.a. att det är lätt och billigt att samla in data och att data om konsumenter har fått ett stort ekonomiskt värde, är någonting som i dagens läge inte längre finns, eller åtminstone inte kommer att göra det inom snar framtid, då denna utveckling fortsätter (Kannan m.fl. 2002). Ur ett sådant perspektiv kan man rimligtvis tänka sig att personer som är medvetna om vilken den framtida utvecklingen riskerar att vara även starkare förespråkar begränsande av övervakning för att försöka få stopp på utvecklingen.

Det enda sättet att garantera integritet online är enligt vissa genom lagstiftning (Acquisti, 2004). Alternativet skulle vara att företag själva reglerade, t.ex. efter press från intressebevakande organisationer eller konsumenter. Andra menar att det finns marknadskrafter som kan motverka denna utveckling. Man tänker sig att då en efterfrågan på privatliv uppstår, kan samma teknologiska utveckling som fick integriteten att "erodera" även användas till att garantera integritet, åtminstone för dem som är villiga att betala för en sådan tjänst (Kannan m.fl. 2002).

### **3.4 Integritetsnormer**

Trots att det moderna samhället borde främja övervakning och informationsinsamling för kommersiellt bruk och således motverka integritetsskydd enligt många observatörer, finns det även de som ser vissa delar av det moderna samhället som understödjande av rätten till privatliv. Alan Westin noterar att demokratiska samhällen tenderar att ha starkare normer för skyddandet av individens privatliv. Enligt honom bildas

integritetsnormer grovt sätt inom två olika typer av samhällsmodeller: auktoritära och demokratiska. Inom auktoritära samhällen ses rätten till privatliv som ett hot mot samhällsordningen och regimen. Inom sådana samhällen övervakar staten noggrant politiska motståndare. Demokratiska samhällen fäster ett mycket större värde vid rätten till privatliv.

Rätten till privatliv ses i demokratiska samhällen som en individuell rättighet som staten enbart i vissa godtagbara syften kan kringgå. Ett sådant syfte är att identifiera antisocialt beteende med målet att bekämpa brott.(Westin, 2003). I enlighet med liberal demokratisk teori är rätten till privatliv sammanbunden med individuell frihet och ett nödvändigt kriterium för att ha ett fungerande demokratiskt samhälle (Colin J Bennett, 1995). För att en individ skall känna sig fri att t.ex. bryta mot sociala beteendenormer eller för att en politisk grupp skall kunna sammanträda öppet kan det anses vara nödvändigt att så sker privat (Solovet, 2003). Ett tydligt exempel på hur man inom politiken tillämpar en sådan princip är vid upprätthållandet av valhemlighet. Sett från ett sådant teoretiskt perspektiv skulle jag kunna tänka mig, att personer som i något avseende avviker från det normala, t.ex. i politiskt avseende, även har en starkare benägenhet att skydda sin integritet online. Social legitimitet är även nära kopplat till integritetsnormer. I regel anses sådana beteenden som är socialt acceptabla även vara privata snarare än offentliga, medan socialt oacceptabla beteenden o andra sidan inte tillåter samma respekt för rätten till privatliv.(Westin 2003, 5).

Då någon uppför sig på ett social oacceptabelt sätt, finns det från myndigheternas och potentiellt allmänhetens sida, en vilja att göra detta beteende offentligt för att t.ex. motverka brott. Den andra sidan av denna situation är hur oliktankare som bryter mot regimen politiska linje riskerar att förföljas om inte rätten till privatliv tryggas.

### **3.5 Rationalitet**

Som vi har sett kan överväganden gällande integritet kopplas till en mängd olika bakgrundsfaktorer. Ett sätt att dela in dessa faktorer, är utgående ifrån vilka antaganden om människan som de grundar sig på. Ett vanligt perspektiv inom forskningen är att utgå ifrån att individer är rationella varelser som fattar beslut utgående ifrån betänkanterna gällande för- och nackdelar hos olika alternativ (Trepte m.fl. 2017). En



teoretisk modell som exemplifierar detta perspektiv är APCO modellen som härstammar från Smith, Dinev och Xu år 2011 (Potoglou m.fl. 2017, 3). APCO står för "Antecedents, Privacy Concerns, Outcomes".

Det är en modell där man ser på vissa individuella faktorer så som kön, ålder samt nivå av "privacy concern" d.v.s. oro gällande integritet, och kopplar detta till vissa resultat såsom delandet av personlig information vid ekonomiska transaktioner ("behavioural intentions such as individuals' willingness to disclose personal information."). Man antar, enligt denna modell, att en människas intentioner är kopplade till ett s.k. "privacy calculus", där individen väger för- och nackdelar mot varandra för att avgöra hur hen bör handla. Detta är i enlighet med "Social exchange theory" d.v.s. utbytesteori (Potoglou m.fl., 2017, 3).

Till näst skall jag behandla tidigare forskning som gjorts för att avgöra vilka faktorer som påverkar människors attityder och beteenden gällande integritet online. Denna tidigare forskning utgår huvudsakligen från människors rationalitet och betydelsen av individuella faktorer. De resultat som presenteras gäller både på orsaker som potentiellt förklarar människors förhållningssätt till integritet och mätningar av den syn som människor har på informationsinsamling och integritet. Avsnittet ger understöd till vissa av de påståenden som gjorts i tidigare avsnitt i detta kapitel gällande sådant som institutionellt förtroende och debatten gällande säkerhet och rätten till privatliv, men lyfter även fram vissa nya förklaringsperspektiv.

### 3.6 Tidigare forskning

I undersökningen: *Internet privacy concerns and beliefs about government surveillance – An empirical investigation* undersöker Tamara Dinev, Paul Hart och Michael R. Mullen (2007) möjliga orsaker till konsumenters villighet att dela med sig personlig information för att kunna utföra ekonomiska transaktioner online.

På motsvarande sätt ser man i studien; *Internet Users' Privacy Concerns and Attitudes towards Government Surveillance – An Exploratory Study of CrossCultural Differences between Italy and the United States*; 2005, på skillnader mellan USA och

Italien som skulle kunna förklara skillnaden mellan människor i dessa länder gällande villigheten att lämna över personlig information vid ekonomiska transaktioner (e-Commerce). Man ser i båda studierna på nivån av "privacy concern" d.v.s. integritetsrelaterad oro, som definieras enligt följande: "Internet privacy concerns refer to perceptions about opportunistic behavior related to the disclosure of personal information submitted over the Internet" (Dinev m.fl. 2008, 218).

Här ses alltså integritetsrelaterad oro främst som en uppfattning om de negativa konsekvenserna av att sådan informationsdelning genomförs. De undersökningar som refereras implicerar ett samband mellan "privacy concerns" och "willingness to provide personal information to transact on the Internet." (Dinev m.fl. 2008; Bellotto Massimo m.fl. 2005). Man ser alltså mindre vilja att dela med sig av personlig information från privatpersoners sida, som en konsekvens av att dessa känner att deras rätt till privatliv inte tryggas.

Därutöver finner man bl.a. att tron att statens övervakning är berättigad, gör en mera benägen att dela med sig av personlig information online. Hur stort behov man anser att det finns av övervakning, har dessutom ett negativt samband till ens integritetsrelaterade oro. Då man anser att det finns flera fördelar med övervakning, såsom högre säkerhet, är man alltså mindre benägen att fokusera vid nackdelarna. Det här verkar handla om hur internetanvändare gör en avvägning mellan risker gällande utelämnande av personlig information till myndigheter och risken att någon tredje part olovligt får tillgång till sådan information. .

I den andra studien, som jämför USA och Italien (Massimo m.fl., 2005), som delvis har samma författare, inkluderas utöver "privacy concern" och "surveillance concern" även faktorer såsom institutionellt förtroende och kollektivism som möjliga förklarande faktorer för hur villiga människor är att dela med sig av personlig information online. Huruvida det som avses är att dessa ytterligare faktorer kan tänkas påverka nivån av integritetsrelaterad oro, som i sin tur påverkar denna villighet eller om det påstås finnas en direkt koppling förblir oklart. Dock finner man betydande skillnader mellan USA och Italien beträffande dessa faktorer och i undersökningens teoridel föreslås de även ha ett samband med de attityder människor har gällande integritet. USA har en högre nivå av institutionellt förtroende medan Italien räknas som ett mera kollektivistiskt

samhälle. Här syftar kollektivism på mindre betoning vid individens betydelse, medan andra enheter såsom familjen har en större betydelse (Massimo m.fl. 2005).

Institutionellt förtroende kan tänkas ha en negativ inverkan på människors tendens att överlämna personlig information vid ekonomiska transaktioner online. Trots att förtroendet för institutioner är lägre i Italien förväntar man sig att italienare är mera benägna att dela personlig information vid sådana transaktioner, därför att en kollektivistisk, familjecentrerad, samarbetsinriktad kultur som Italien inte gynnar integritetsskydd som norm: "The concept of privacy is related to the extent that individualism is sought after and reinforced in a culture" (Massimo m.fl. 2005). Därav följer undersökningens första hypotes: "Internet privacy concerns are negatively related to e-commerce use for both cultures, the relationship being stronger for the individuals in the U.S". Man tänker sig alltså att "privacy concern" precis som i undersökningen *"Internet privacy concerns and beliefs about government surveillance – An empirical investigation"* (Dinev m.fl. 2008) påverkar villigheten att överlämna personlig information vid ekonomiska transaktioner online negativt, och att individualism stärker denna tendens.

Vad det gäller upplevt behov av statlig övervakning, t.ex. med syftet att förhindra cyberbrottslighet, antas amerikaner anse att behovet är större än vad italienare gör, på grund av den effekt terroristattacken 11.9.2001 har haft och på grund av att amerikaner har ett högre institutionellt förtroende. "More specifically, in our model, it is defined as the perception that the government needs greater access to personal information and greater authority to conduct surveillance of Internet transactions" (Massimo m.fl. 2005). Denna undersökning nämner även "government intrusion concerns" som en faktor som påverkar attityden människor har till att dela personlig information vid ekonomiska transaktioner online. Denna faktor handlar om att statens övervakning går för långt. Människor kan vid en viss nivå av övervakning anse att de är obekväma med att bli övervakade, dock utan att detta upplevs som en kränkning av deras rätt till privatliv. Denna distinktion verkar tvivelaktig. Som jag själv ser det borde varje fall av "government intrusion concern" även kunna definieras som ett fall av "privacy concern", medan det omvända inte gäller. Dessa undersöks dock som två skilda faktorer och antas ha ett samband med varandra. "Government intrusion concerns" antas även påverka viljan att lämna ut personlig information vid ekonomiska transaktioner online på ett negativt sätt (Massimo m.fl. 2005). Det antas alltså finnas ett positivt samband

mellan hur stort någon anser att behovet av övervakning är och viljan att dela med sig av personlig information vid ekonomiska transaktioner online. Från detta resonemang följer följande hypotes:

“Justification for government security is positively related to e-commerce use, the relationship being stronger for U.S. individuals”. Denna hypotes bekräftas delvis i undersökningens analysdel. Förhållandet är klart starkare för amerikaner. Sambandet mellan dessa variabler är dock inte statistiskt signifikant för italienare.

Författarna föreslår att det är möjligt att dessa faktorer inte påverkar varandra inom den italienska populationen. För “government intrusion concerns” och “privacy concerns” finns det även klara skillnader mellan Italien och USA. “Government intrusion concerns” verkar inte påverka amerikaner i deras attityd till utelämnande av personlig information vid ekonomiska transaktioner online, medan denna inverkan är stark för italienare. Vad det gäller “privacy concerns” är kopplingen dock starkare för amerikaner än för italienare. Resultatet kan kanske förklaras av att individualism är starkare i USA, vilket i sin tur hänger ihop med att integritet som koncept inte har en starkare roll i det amerikanska samhället.

Undersökningen visade dessutom att det hos amerikaner finns ett samband mellan “government intrusion concern” och “privacy concern”. Amerikaner som är mera oroliga över statlig övervakning, är även mera oroliga över upprätthållande av integritetsskydd generellt sätt, samtidigt som detta inte leder till förändrat beteende online, på basis av undersökningen.

Att människor anser att det finns ett behov av statlig övervakning sammanhänger, kanske inte så överraskande, med att de är mera villiga att lämna ut personlig information. Inte heller verkar det speciellt överraskande att personer med mera “privacy concern” är mindre benägna att lämna ifrån sig sådan information. Dessa sambands styrka eller till och med deras förekomst verkar dock variera på basis av vissa kulturella faktorer. Vad som framförallt framstår som intressant i denna typ av undersökningar, är vilka bakgrundsfaktorer som skulle kunna tänkas förklara variationen i dessa samband.

Allvarliga hot mot den allmänna säkerheten, så som terrorist-attentat, är en bakgrundsfaktor till människors attityd till statlig övervakning, som verkar vanlig inom litteraturen. Allmänheten är i krissituationer villiga att avstå från en del av sitt

integritetsskydd med syftet att nå högre säkerhet. Dock krävs det att människor har förtroende för de institutioner som skall utföra övervakningen. Individualism och kollektivism kan även tänkas påverka vilken betydelse integritet ges och hur människor förhåller sig till att lämna ut personlig information online.

Studien: “Public Feeling on Privacy, Security and Surveillance” (Bakir m.fl. 2015, 4-5 ) finner att det verkar finnas en skillnad mellan hur myndigheterna ser på övervakning och den brittiska allmänhetens syn. Dels har myndigheter och allmänheten olika syn på vad som bör kategoriseras som “mass surveillance” d.v.s. massövervakning, dels har de brittiska myndigheterna en något annorlunda syn på vilken balans den brittiska allmänheten anser att bör finnas mellan privatskydd och övervakning, än den syn som opinionsundersökningar visar att allmänheten har. Myndigheterna anser att den allmänna opinionen är den, att övervakning och de mål som de anser kan nå genom övervakning, är klart viktigare än integritetsskydd, “we do not subscribe to the point of view that it is acceptable to let some terrorist attacks happen in order to uphold the individual right to privacy—nor do we believe that the vast majority of the British public would’ (Intelligence and Security Committee, Privacy and Security: A Modern and Transparent Legal Framework. House of Commons [12 March]. 2015: 36).” Denna åsikt går inte att se inom de opinionsundersökningar som gjorts för att mäta allmän opinion.

Enligt “Digital Citizenship and Surveillance Society(DCSS)Study” anser den brittiska allmänheten att “Bulk Data Collection”, som är massinsamling av metadata, är en form av massövervakning medan de brittiska myndigheterna menar att det inte är det, på grund av att datainsamlingen är selektiv och man saknar vilja och resurser att behandla data från den brittiska allmänheten i dess helhet (Bakir m.fl. 2015, 6-8).

Orsaker till att det är fråga om massövervakning, som angetts av den brittiska allmänheten, är bl.a. avsaknaden av medgivande, avsaknaden av anonymitet, tvivel angående behovet av sådan datainsamling och de möjligheter att identifiera någon som metadata skapar. Dessa attityder verkar alla ha en koppling till uppfattningen att de brittiska myndigheterna inte går att lita på beträffande användandet av sin övervakningskompetens. Detta framgår även av andra delar av denna rapport, så som

gällande studien: "Surveillance, Privacy and Security (SurPRISE) Study" från år 2014 (Bakir m.fl. 2015, 8-11).

Trots att såväl den brittiska allmänheten som européer generellt sätt uppfattar att det finns ett behov av att använda övervakningsteknologier för att uppnå mera säkerhet, anser en större del av den brittiska befolkningen att myndigheterna inte är tillförlitliga när det kommer till att inte missbruka sina makt, än den andel som gör det. År 2015 frågades den Brittiska allmänheten: "if GCHQ (Government Communications Headquarters) did have the resources and capability to intercept/collect the internet-based communications of everyone could they be trusted not to abuse this ability?" En majoritet av de som tog ställning på 42 % svarade nekande, medan 34 % ansåg att de kunde lita på GCHQ . Enligt samma mönster är andelen EU-medborgare som tror att maktmissbruk av övervakningsbefogenheter förekommer större än de som inte tror det (Bakir m.fl. 2015, 7-8).

Dessutom är det även en majoritet som anser att användningen av sådan teknologi är ett hot mot grundläggande mänskliga rättigheter. Majoriteten av medborgarna inom EU anser att det finns en risk att dessa rättigheter kränks. Det verka finnas en viss kognitiv dissonans inom den europeiska och brittiska allmänheten. Givet att man trots allt vill ha ökad övervakning, åtminstone inom en del områden, verkar det betyda att människor i allmänhet är intresserade av att offra en del av sin integritet för att få mera trygghet. Betydelsen av att värna om mänskliga rättigheter kanske inte väger lika tungt som behovet av säkerhet, antiterrorism och brottsbekämpning. Så som i undersökningar gjorda om USA, finner man i de undersökningar som gjorts gällande den brittiska befolkningen att den allmänna oron gällande integritetsskydd eller nivån av "privacy concern" har stigit under de senaste åren, exempelvis enligt studien: *Digital Citizenship and Surveillance Society (DCSS) Study: Quantitative Findings*. (Bakir m.fl. 2015, 8).

I samma undersökning tar man upp vilken betydelse Edward Snowdens informationsläcka gällande amerikanska myndigheters övervakning haft för den allmänna opinionen i Storbritannien. Det verkar som om denna incident kan ha haft en inverkan. 60 % sade att de var mera oroliga över sin nivå av integritet än för ett år sen, då de frågades ett år efter att Snowdens informationsläcka hade inträffat. Dock har nivån av oro stigit från år till år, så denna inverkan är inte uppenbar. Därutöver ansåg en majoritet att Snowdens informationsläcka var en bra sak, vilket även kan tänkas säga

något om den brittiska allmänhetens attityd till integritetsskydd. Det visar att man upplever att den oro allmänheten har gällande övervakning och minskade möjligheter till privatliv, bekräftas av personer såsom Edward Snowden. En sådan incident, som Snowdens informationsläcka till media, kan möjligtvis skapa ytterligare oro gällande trygghet av rätten till privatliv samt leda till minskat förtroende för myndigheter.

Då man analyserar vilka demografiska faktorer som sammanhänger med "privacy concern" visar det sig att ålder spelar en klar roll. I flera studier som gjorts finner man en positiv koppling mellan ålder och hur positivt inställd en person är till användning av "security-oriented surveillance technologies", d.v.s. övervakningsteknologi (undersökningarna surPRISE och DCSS), samt en negativ koppling mellan hur orolig man är över att ens rätt till privatliv blir kränkt och ålder. Då man ser på avvägningen mellan behovet av övervakning och skyddande av integritet i förhållande till myndigheter, är det endast personer över 60 som vill se mera övervakning på bekostnad av integritet. Det går klart emot de Brittiska myndigheternas uppfattning av allmän opinion i denna fråga. Överlag är denna åldersgrupp även mera positivt inställda till statlig övervakning. Gällande frågor som huruvida myndigheter borde få tillgång till information om vad internetanvändare gör online eller huruvida det var acceptabelt att GCHQ tagit data direkt från fiber-kablar för att samla in information om människor oberoende av misstankar om brott, är personer över 60 den enda ålderskategori där en majoritet anser att sådan övervakning är berättigad.

Därutöver finns det en koppling mellan etnicitet och oro över statliga maktmissbruk inom övervakning. Personer som tillhör en minoritetsgrupp är mera oroliga över att maktmissbruk av myndigheternas övervakningskapacitet sker och mera oroliga över att deras rätt till privatliv blir kränkt.

I denna undersökning finner man alltså ytterligare bakgrundsfaktorer till oro över potentiella maktmissbruk av övervakningskompetens. Ålder verkar ha ett klart samband inom den brittiska populationen, men även händelser som Edward Snowdens informationsläckage kan tänkas vara avgörande för allmän opinion. Ett gap som finns inom mycket av forskningen gällande människors preferenser för privatliv och informationsinsamling, är att många av de undersökningar som har gjorts ser på ekonomiska transaktioner online (e-commerce) och fokuserar på informationsinsamling och informationsdelning som företag gör (Potoglou m.fl. 2017, 2).

Inställning till företags rätt till sådana aktiviteter kan naturligtvis anses vara en politiskt relevant fråga, men om man är intresserad av att se på vilka preferenser människor har i förhållande till sådan informationsinsamling i allmänhet, inkluderat statlig övervakning, kan det behövas ett annat mått.

En aktör som har exceptionella förutsättningar för att samla in personliga data om internetanvändare är s.k. ISP:s. ISP står för internet service provider. Det är företag som gör det möjligt för internetanvändare att få tillgång till internet. Då människor använder internet och besöker olika hemsidor, finns det en möjlighet att lagra data om vilka hemsidor de besöker. Ett sätt att mäta det förhållningssätt människor har gällande sådan informationsinsamling, som ett forskarteam vid Rand Corporation använt sig av då de analyserat Europeiska medborgares attityder inom det här området, är att ställa testpersoner inför ett konsumtionsval. Om du som konsument skall välja mellan ett antal olika ISP:s, vars policy gällande insamlande, sparande och utlämnande av data skiljer sig åt och om olika alternativ dessutom kostar olika mycket, är du då beredd att betala ett högre pris för att skydda din personliga information?

I den studie detta forskarteam utförde, använde man alltså hypotetiska ekonomiska beslut som ett sätt att försöka avgöra hur viktigt det är för amerikaner att undanhålla personliga data. Analysen som gjordes av de insamlade data, visar hur vissa socioekonomiska faktorer har ett positivt samband med hur stark aversion någon har till att ISP:s samlar in och sparar information om sina kunder. Att vara man och äldre har till exempel ett visst positivt samband, enligt denna studie. Detta samband går ihop med de forskningsresultat som presenterades i "Public Feeling on Privacy, Security and Surveillance", där ålder hänger samman med större tolerans för övervakning och mindre oro över att ens rätt till privatliv blir kränkt.

I en annan studie med liknande ändamål och samma datamaterial, vid namn "Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study" (Potoglou m.fl. 2017) undersöker man även valet av ISP som ett sätt att avgöra människors preferenser gällande integritetsskydd. Den allmänna opinionen i EU verkar vara emot lagrande och användande av data gällande internetaktivitet av "internet service providers". Då EU-medborgare ställs inför valet av ISP och det som skiljer de olika alternativen åt är i vilken utsträckning information om vad de gör på nätet, vilka webbsidor de besöker, vem de kommunicerar med o.s.v.



lagras och potentiellt delas med företag eller myndigheter, är den allmänna trenden, att européer vill minimera sådan informationsbehandling.

EU-medborgare föredrar att ISP:s inte lagrar någon information alls om deras internetanvändning. Denna slutsats grundar sig på hur de svarande ställs inför ett val bestående av fem olika hypotetiska ISP-alternativ, som lagrar olika stora mängder information om vad internetanvändare gör. Det är kanske rätt så lätt att förstå vilka preferenser EU-medborgare har, givet hur hög nivå av "privacy concern" de rapporterar.

Då man jämför olika länder finner man att den finska befolkningen är exceptionellt starkt emot att sådan informationslagring genomförs (Potoglou m.fl. 2017, 8). Det finns även ett visst samband mellan denna preferensdimension och kön. Kvinnor hade i allmänhet en svagare preferens för att ingen information om internet aktivitet sparas och valde därmed mera sannolikt ett alternativ där åtminstone någon information sparas.

Undersökningen visar även att EU-medborgare föredrar att ISP:s inte delar information med polisen. Denna aversion var starkare för större områden, då alternativen gick från "police in homecountry" till "police worldwide" (Dimitris Potoglou m.fl. 2017, 9-10). Detta gällde trots tilläggsvillkoret "if seen needed by a judge/court". Man frågade dessutom undersökningsdeltagarna när en ISP kan/tillåtas ge polisen rätt till kontinuerlig övervakning av internetanvändare. I denna fråga föredrog svarande i allmänhet att ge denna rätt med en arresteringsorder. Personer över 65 var mindre emot kontinuerlig övervakning, både med en arresteringsorder och utan. Samma grupp var även mera intresserade av "privacy enhancing services" än andra grupper. Så som i andra studier som undersökt inställning till integritetsskydd och övervakning, visar denna undersökning alltså att äldre personer tenderar att ha högre tolerans i förhållande till övervakning (Potoglou m.fl. 2017, 10).

### **3.7 Hypoteser**

Dessa olika undersökningar och teorier om integritet erbjuder en mångfald av faktorer som kan förklara människors attityd till integritet online. Det är dock viktigt att komma ihåg att olika faktorer opererar på olika nivåer. Vissa faktorer, så som ålder eller

förtroende för myndigheter, är faktorer på individnivå medan andra, så som hur individualistisk kulturen i ett land är, är faktorer på systemnivå, i detta fall landnivå. Jag planerar att göra mina analys om faktorer på individnivå, eftersom det data- material jag har tillgång till tjänar ett sådant syfte bättre.

Utgående ifrån de teorier om ämnet jag bekantat mig med och presenterat i teoridelen av denna avhandling, kan jag bilda ett antal preliminära hypoteser som utgångspunkt för analysdelen av avhandlingen. För det första, verkar det som om ålder är en individuell faktor som förklarar, eller åtminstone korrelerar med den attityd olika människor har till vissa former av informationsinsamling. Beträffande myndigheters övervakning, verkar det finnas ett positivt samband mellan ålder och hur positivt någon förhåller sig till övervakning. Det visar tidigare studier (Bakir 2015; Potoglou 2017). Därmed förväntar jag mig hitta ett liknande samband i de datamaterial jag själv kommer att analysera. Min första hypotes är alltså:

**H1: Ålder har ett negativt samband till en individs oro gällande myndigheters övervakning på internet.**

Här handlar det alltså specifikt om myndigheters övervakning, snarare än informationsinsamling av organisationer i allmänhet.

En annan faktor som dyker upp i litteraturen både uttryckligen och implicit är hur människors förtroende för myndigheter och möjligtvis även företag, påverkar hur de förhåller sig till informationsinsamling av personliga data. Jag tänker mig att människor som har mindre förtroende för myndigheterna anser att risken är högre att den information myndigheterna samlar in används på ett sätt som skadar dem. Då den amerikanska staten hävdar att den utför informationsinsamling angående elektronisk kommunikation med amerikanska invånares intresse i åtanke, kommer alltså personer med lägre institutionellt förtroende tendera att vara mera skeptiska till att detta stämmer. Det gör dem i sin tur mindre villiga att understöda sådan informationsinsamling. Min andra hypotes är således:

**H2: Högre förtroende för myndigheter har ett negativt samband till en individs oro gällande myndigheters övervakning på internet.**

Westin (2003) gällande integritetsnormer, demokrati och social legitimitet, samt Bennett (1995) gällande integritet och demokrati, ger mig även anledning att föreslå

följande: Personer som är politiskt avvikande är mera negativt inställda till att personlig information om dem samlas in online. Med avvikande menar jag att de skiljer sig tydligt från den politiska mitten gällande sina värderingar och åsikter. Ett annat sett att formulera detta skulle vara: Det finns ett positivt samband mellan avståndet till den politiska mitten från en individs position på en politisk höger-vänsterskala och deras aversion mot att personlig information om dem samlas in online.

Om en person avviker beteendemässigt och beträffande sina värderingar, kan det hända att denna avvikelse är socialt oacceptabel. Det kan i sin tur betyda att de beteenden som denna person utför och innehavande av de värderingar som personen har, riskerar att leda till vissa negativa sociala påföljder. I enlighet med liberal demokratisk teori kan individer i ett demokratiskt samhälle känna sig fria att bryta mot sociala beteendenormer enbart ifall de har rätt att göra detta privat (Colin J Bennett, 1995). Utgående ifrån dessa antaganden drar jag slutsatsen att personer som har åsikter som är politiskt avvikande har ett större behov av att deras rätt till privatliv tryggas, vilket inkluderar deras rätt till privatliv på internet. Därmed kommer de att vara mera negativt inställda till övervakning av myndigheterna online.

Min hypotes är därmed:

**H3: Det finns ett positivt samband mellan hur politiskt avvikande någon är och denna individs oro gällande myndigheters övervakning på internet.**

Vad tidigare forskning även visar är att händelser på samhällsnivå ss. Terrorist/attentat, möjligtvis påverkar människors villighet att avstå från sin integritet på internet (Westin 2003; Massimo 2005). Ett exempel är den amerikanska statens övervakning efter terroristattentatet 2001 och människors medgivande till att utöka statliga övervakningsbefogenheter. Då dessa befogenheter utökades var den officiella motiveringen att mera övervakning skulle bidra till bättre förutsättningar för att motverka framtida liknande händelser. Terroristattentat och understöd för mera övervakning som en säkerhetsåtgärd har alltså inte enbart varit ihopkopplade tidsmässigt, då allmänheten sett hotet av terrorism som en motivering till ökad övervakning, utan även i den retorik som framförts av förespråkare för större övervakningsbefogenheter, både direkt efter sådana händelser och senare då sådan övervakning stött på kritik. Den debatt som uppstod efter Edward Snowdens informationsläckage är ett tydligt exempel. Om man kopplar ihop statlig övervakning

med terrorismbekämpning, verkar sannolikt att man är mera tolerant i förhållande till statlig övervakning online. Jag tänker mig att en person som hör mera om att staten övervakar, med det uttryckliga syftet att motverka terrorism, mera sannolikt kommer att göra den kopplingen. En möjlig femte hypotes är därmed:

**H4: Kännedom om statlig elektronisk övervakning med syfte att motverka terrorism har en negativ effekt på en individs oro gällande myndigheters övervakning på internet.**

Kännedom handlar i detta sammanhang om hur mycket någon har hört om ämnet, snarare än kunskap om ämnet. En person som är välbekant med ämnet kan naturligtvis vara skeptisk till huruvida denna övervakning är legitim, men det verkar sannolikt att sådan information generellt sätt får personer att uppfatta övervakning som mera legitim. Det skulle även understöda en hypotes som baserar sig direkt på tidigare forskning, som gäller sambandet mellan terroristattentat och attityd till statlig övervakning, nämligen:

**H5: Terrorist-attentat leder till att individer i det land attentatet sker blir mera positivt inställda till statlig övervakning. Denna effekt avtar över tid.**

Denna sista hypotes skulle vara intressant att undersöka. Dock möjliggör det datamaterial jag har inte testande av hypotesen, utan denna förblir en slutsats på basis av tidigare forskning. Till näst kommer jag att redogöra för hur mina hypoteser testas genom statistisk analys och vilka metodologiska antaganden som denna analys grundar sig på. Det inkluderar vilket data jag använder mig av, hur jag mäter de variabler analysen inbegriper, samt valet av statistisk analysmetod.

## 4. Forskningsdesign

Människors förhållningssätt till integritet online, i termer av hur de förhåller sig till informationsinsamling om dem, är alltså intresset för min undersökning. Vad jag är intresserad av att se på i den empiriska delen av min avhandling är vilka faktorer som uppvisar ett samband med detta förhållningssätt. Förhållningssätt till informationsinsamling online kan som variabel delas upp i olika mera specifika variabler t.ex. på basis av vilken slags information som samlas in. Det finns flera sorters organisationer som samlar in information online om privatpersoner och som därmed är av betydelse för integritet på internet. Jag kommer att avgränsa mig till att se på myndigheters informationsinsamling och är intresserad av personlig information i största allmänhet.

Jag kommer att analysera sambandet mellan attityden till integritet och vissa andra attityder människor har samt sambandet till vissa socioekonomiska faktorer. Dessa andra attityder som bildar två av mina oberoende variabler är hur stort människors förtroende för myndigheter är och hur politiskt avvikande de är. Vad jag är intresserad av gällande politisk avvikelse är de flera olika attityder som tillsammans avgör var någon placerar sig på en politisk höger-vänsterskala och hur mycket denna placering avviker från den politiska mitten. Därutöver kommer jag att analysera sambandet mellan hur mycket någon säger att de hört om statlig övervakning med syfte att motverka terrorism och deras attityd till övervakning online. De socioekonomiska faktorerna är kön, ålder och utbildningsnivå. Valet av population i min undersökning är den amerikanska befolkningen. Min forskningsfråga är därmed mera specifikt: Vilka faktorer förklara variationen i förhållningssätt till integritet online hos amerikaner?

Jag kommer att utföra en statistiska analys av sambandet mellan amerikaners förhållningssätt till informationsinsamling online och tre andra variabler som berör deras attityder och uppfattningar med syftet att försöka förklara varför olika amerikaner har olika attityd till att de amerikanska myndigheterna samlar in information om dem på internet. Enbart förekomsten av ett sådant samband är dock inte tillräckligt för att man skall kunna påstå att dessa oberoende variabler förklarar variationen hos min beroende variabel, vilket jag skall gå närmare in på längre fram i detta kapitel.

Som utgångsläge för mitt val av fall hade jag först och främst ett intresse av att studera individer som är aktiva internetanvändare. Orsaken är kanske rätt så uppenbar. Personer som inte använder internet, har ingen internetaktivitet som myndigheter kan övervaka och ingen onlinekommunikation att skapa metadata gällande. Jag är dessutom intresserad av individer som lever i länder där staten har betydande kapacitet för övervakande av privatpersoner på internet. Om man studerar attityden till statlig övervakning online måste sådan övervakning förstås förekomma och inte vara trivial. Om den statsmakt vars invånare jag valt att studera t.ex. enbart utförde övervakning av sina medborgare i specialfall p.g.a. bristande teknisk kapacitet, och den totala informationsinsamlingen var väldigt begränsad, skulle det inte finnas så mycket för respondenterna i en undersökning om statlig övervakning att ha en attityd i förhållande till.

USA uppfyller båda dessa krav. Amerikanska invånare är aktiva internetanvändare och den amerikanska staten har betydande kapacitet och vilja att ägna sig åt massövervakning online. Den samhällsutveckling som sker gällande övervakning och privatliv i informationsteknologins tidsålder är kanske som allra tydligast i USA. Då jag sökt efter data har det dessutom varit USA jag hittat bäst data om, vilket även naturligtvis påverkat mitt val.

## **4.1 Data**

Det data jag använder i min analys kommer från en enkätundersökning som gjorts av Pew Research Center som genomförts med hjälp av en onlinepanel med namnet KnowledgePanel. Denna onlinepanel har skapats av en organisation vid namn GfK Group. De personer som deltog i Pew Researchs online privacy panel bildades som en underpanel av denna panel. I respondentundersökningar, såsom enkätundersökningar av den här typen, är man inte intresserad av att samla in fakta som deltagarna har, utan man vill lära känna vilka idéer och attityder dessa har inom något ämne. (Esaiasson m.fl. 2017).

I enkätundersökningar använder man sig av standardiserade frågor så att alla respondenter som deltar svarar på samma frågor. De frågor man ställer är preciserade och svarsalternativen är fasta. Vad man mäter är alltså frekvensen av hur ofta olika svarsalternativ har valts (Esaiasson m.fl. 2017). Då man bjuder in deltagare är urvalet i

regel slumpmässigt för att deltagarna skall bilda ett så representativt urval som möjligt av befolkningen. På så vis hoppas man kunna beskriva hur vanliga olika åsikter och attityder är inom befolkningen i dess helhet, t.ex. hur vanligt är det att ha ett högt institutionellt förtroende inom den amerikanska befolkningen? Pew Researchs undersökning är en enkätundersökning som man gjort via internet. Det är dessutom en panelundersökning, så deltagarna i undersökningen har svarat på flera enkäter, i detta fall fyra.

Gfk Group bjöd in 1,537 personer att delta i fyra enkäter som handlar om “current issues, some of which relate to technology” och därutöver att möjligtvis delta i fokusgrupper. 935 personer svarade på inbjudan, varav 607 gick med på att delta (Pew Research Center, 2014). Jag kommer att använda mig av data från två av de enkäter som dessa människor deltog i, den första och den tredje. Den första ägde rum 10.01.2014–27.01.2014, den tredje 26.11.2014–03.01.2015. I den tredje enkäten deltog 475 av de 607 personer som ursprungligen gick med på att delta. Jag kommer alltså enbart att använda data om personer som deltog i båda dessa enkäter. Syftet Pew Research Center säger sig ha med undersökningen är att utreda amerikaners övervakningsrelaterade uppfattningar och beteenden efter att den amerikanska statens olika övervakningsprogram kommit till allmän kännedom på grund av Edward Snowden i juni 2013.(Pew Research Center, 2014).

## 4.2 Urval

Då man gör en observationsstudie av det här slaget är man intresserad av att kunna beskriva den befolkning man undersöker i sin helhet. För att kunna göra detta skulle man i princip kunna se på alla individer i populationen, men i praktiken har man inte alltid möjlighet. Jag undersöker den amerikanska befolkningen och de personer som deltog i Pew Researchs undersökning bildar ett stickprov av denna befolkning. Givet att ett stickprov tas slumpmässigt kommer de värden som gäller för stickprovet, t.ex. andelen personer som är kvinnor, med en viss sannolikhet att finnas inom ett visst avstånd från det värde som gäller för populationen i dess helhet (Lantz, 2011). Då man gör en intervallskattning påstår man att det sanna värdet, alltså värdet för hela populationen, med en viss sannolikhet finns inom ett intervall som bildas av motsvarande värde för stickprovet och en felmarginal. Detta intervall kallas för ett konfidensintervall och dess bredd har en positiv inverkan på hur stor sannolikheten är

att intervallskattning stämmer, d.v.s. hur hög konfidensnivån är (Lantz, 2011). Det som dessutom påverkar konfidensnivån är hur stort stickprovet är. Ett större stickprov ger en högre konfidensnivå, eller annorlunda uttryckt: om stickprovet är större och konfidensnivån är den samma, leder det till att konfidensintervallet är mindre. Stickprovets storlek kommer i mitt fall att vara 475 fall stort, eftersom enkättagarna som svarat på samtliga frågor jag använder mig av från enkätundersökningen, är så många till antalet. Konfidensnivån som man typiskt sätt använder sig av i statistiska undersökningar brukar vara på 95- eller 99-procentsnivån. Om konfidensnivån är 99-procent, säger man att undersökningens signifikansnivå är på 1 %-nivån. Hur stor felmarginalen kommer att vara d.v.s. hur brett intervallet i min intervallskattning av olika värden kommer att vara, påverkas av vilken konfidensnivå jag använder mig av och storleken på mitt stickprov (Lantz, 2011).

Då man gör en statistisk undersökning försöker man ofta testa huruvida någon viss hypotes stämmer. Om man undersöker amerikaners attityd till integritet på internet, kan man t.ex. vilja testa huruvida en majoritet har en negativ inställning till datainsamling av personliga data av myndigheterna. En hypotes som man arbetar med skulle alltså kunna vara, att en majoritet har en negativ attityd.. En nollhypotes är ett koncept som blir användbart i detta sammanhang. Nollhypotesen påstår negationen till det hypotesen man vill testa påstår, som i sin tur kallas mothypotes. I ovanstående exempel skulle nollhypotesen alltså påstå att det inte är en majoritet av den amerikanska befolkning som förhåller sig negativt till sådan datainsamling. För att nollhypotesen skall kunna förkastas måste sannolikheten för att den stämmer givet det stickprov man har, kallat p-värde, vara lägre än signifikansnivån (Lantz, 2011). Om man har en hypotes som påstår att majoriteten av den amerikanska befolkningen inte vill att myndigheterna samlar in data om vad de gör på internet och man väljer en signifikansnivå på 5 %, måste alltså p-värdet vara lägre än 5 för att man skall kunna förkasta nollhypotesen d.v.s. att det inte är en majoritet som har den åsikten.

Uträknande av ett p-värde är även möjligt för hypoteser gällande korrelation. Jag kommer att utföra en logistisk regressionsanalys. Vid en sådan analys testas huruvida variablerna i analysen har ett samband. Nollhypotesen skulle då i regel påstå att variablerna inte har något samband och p-värdet anger hur sannolikt detta är, givet att stickprovet visar att variablerna har ett samband.



Då man strävar efter att säga något om populationen i dess helhet på basis av det data man har, är det viktigt att vara medveten om vilken innebörd sådant som p-värde och signifikansnivå har. När man undersöker ett stickprov av en population finns det allt som oftast en risk att det som gäller för stickprovet, inte gör det för hela populationen. Detta blir mera sannolikt ifall urvalsprocessen inte är slumpmässig av någon anledning. Det kan till exempel vara så att personer som är villiga att delta i en enkätundersökning, så som den Pew Research gjort, tenderar att svara annorlunda på någon av de frågor som de blivit ställda än vad människor i allmänhet skulle göra (Esaiasson m.fl., 2012). Det skulle vara ett exempel på bristande validitet. Till näst skall jag gå närmare in på vad validitet innebär, samt utreda innebörden hos två andra begrepp som är centrala då man gör en empirisk undersökning: operationalisering och reliabilitet.

### 4.3 Operationalisering, validitet och reliabilitet

För att operationalisera mina variabler är det nödvändigt att först säkerställa att jag nått klarhet gällande innebörden hos mina begrepp (P. M. Kellstedt, G. D Whitten, 2013, s. 99). Förhållningssätt till integritet kan förstås tolkas på olika sätt, så för att vara mera specifik är jag intresserad av den attityd människor har till att personlig information som genereras då de använder internet eller laddas upp av dem, samlas in. I detta sammanhang handlar alltså integritet om hur mycket olika aktörer känner till om dem genom insamling av data online. Med personlig information menar jag information som på något sätt handlar om en individ, t.ex. vilka hemsidor denna person besöker.

Denna tolkning är härledd från ett antal olika definitioner av integritet eller engelskans *privacy*, som jag behandlat i teoridelen. Det första steget för att nå från en abstrakt teoretisk definition, till ett begrepp som kan mätas, har i mångt och mycket handlat om att avgränsa mitt begrepp. I en sådan process är det viktigt att inte eliminera sådant som är en del av det som begreppet nödvändigtvis måste innehålla, för att fortfarande vara samma begrepp. När jag talar om vad jag mera specifikt menar med integritet, måste denna innebörd med andra ord fortfarande vara en form av integritet, annars riskerar min operationalisering att lida av dålig begreppsvaliditet.

Om jag använder mitt specificerade begrepp till att genomföra en operationalisering för att kunna mäta förekomst av det fenomen som intresserar mig, och jag har ändrat om

begreppet då jag gjort mina avgränsningar, kommer det att medföra ett systematiskt fel i min undersökning. Systematiska fel av det här slaget är i grund och botten vad begreppsvaliditet handlar om (Esaiasson m.fl. 2012). I min operationalisering kopplas mina begrepp till vissa frågor som deltagarna i Pew Researchs enkät har blivit ställda. Här finns förstås även en risk att problem gällande begreppsvaliditet uppkommer. Man kan säkert använda sig av många olika frågor för att avgöra hur någon förhåller sig till att information samlas in om dem gällande deras internetaktivitet. Det sätt som jag har valt att operationalisera mina begrepp på är genom att resonera mig fram till den bästa operationaliseringen, vilket är en möjlig strategi för operationaliserande (Esaiasson m.fl. 2012). Denna strategi kräver att man demonstrerar en logisk koppling mellan den operationella indikatorn och det abstrakta begrepp man försöker mäta. Om mina resonemang är hållbara borde jag alltså ha uppnått god begreppsvaliditet,

Det är viktigt att hålla i tankarna, då man formulerar sina frågor, att inte ställer frågor som är ledande. Ett exempel på detta problem är hur människor har en tendens att hålla med då frågan de ställs är en samtycksfråga d.v.s. en fråga där man som svarande kan välja mellan att hålla med om ett påstående eller vara emot det. Därutöver måste frågan vara formulerad på ett begripligt sätt. Enligt författarna av metodpraktikan är det nödvändigt att uppnå följande 6 krav för att en fråga skall vara tillräckligt lättbegriplig: 1) Frågan får inte vara för komplicerad 2) Undvik svåra ord 3) Undvik vaga ord 4) Ställ en tillräckligt kort fråga 5) Fråga en sak i taget 6) Undvik negationer (Esaiasson m.fl., 2012).

Då man har fasta svarsalternativ, som i Pew Researchs undersökning, är det dessutom viktigt att alternativen är uttömmande och ömsesidigt uteslutande (Esaiasson m.fl., 2012). Det skall alltså gå att hitta ett svarsalternativ som passar den åsikt man har som respondent, oberoende av vilken åsikt man har och det skall inte finnas flera svarsalternativ som helt eller delvis har samma betydelse, så att endast ett alternativ passar.

Hur frågorna mera specifikt är formulerade är av betydelse för huruvida man når god begreppsvaliditet och en mätning som har tillräcklig reliabilitet. Vad man märkt vid undersökandet av människors åsikter är att även små variationer i hur en fråga är formulerad kan skapa variation i hur människor svarar. En lösning på denna problematik är att, istället för att fokusera på nivåskattning d.v.s. vilken andel av

populationen som placerar sig i någon viss kategori, fokusera på skillnader över tid eller skillnader mellan grupper. Dessa skillnader borde inte vara lika känsliga för frågors formulering (Esaiasson m.fl., 2012).

Då jag utför min statistiska analys kommer jag att jämföra olika delar av befolkningen med varandra, indelade på basis av mina oberoende variabler, med avseende på min beroende variabel. De skillnader som finns mellan människor som t.ex. har ett högre förtroende för myndigheter och de med ett lägre förtroende, gällande deras attityd till integritet online, borde alltså inte påverkas allt för mycket av de formulering Pew Research har valt då de frågat människor om deras attityd till integritet online.

Vad det gäller möjligheten att trots ovannämnda osäkerhet hos nivåskattning, göra en sådan, identifierar författarna av metodpraktikan (Esaiasson m.fl., 2012) tre stycken kriterier man kan försöka uppnå. För det första: användandet av flera olika frågor som mäter samma attityd, för att avgöra hur känsligt svarande är för förändringar i frågans formulering. För det andra är det värt att lita mera på en nivåskattning då frågan man ställer handlar om faktiskt agerande snarare än abstrakta tankekonstruktioner. För det tredje kan man lita mera på en nivåskattning gällande människors åsikter om det ämne frågan handlar om har funnits med länge i den offentliga debatten. Min undersökning uppfyller tyvärr inget av dessa tre kriterier. Jag använder endast en fråga per variabel för att få ett mått. De frågor jag använder mäter människors attityd i förhållande till någonting, inte hur de agerar. Integritet online har inte funnits med speciellt länge i den offentliga debatten och är det fortfarande bara sporadiskt. Dessa svagheter blir jag tvungen att hålla i tankarna då jag ser på hur värdet på min beroende variabel fördelar sig inom den amerikanska befolkningen (Esaiasson m.fl., 2012).

Enligt Esaiasson m.fl. kan validitetsproblematiken i en undersökning beskrivas med formeln: begreppsvaliditet + reliabilitet = resultatvaliditet.

Vad det gäller den andra variabeln i denna formel har jag begränsade möjligheter till påverkan. Jag har inte samlat in mitt data själv utan använder data som samlats in av organisationen Pew Research Center. Det är förstås fullständigt möjligt att forskarna vid detta center har gjort slarvfel eller andra osystematiska fel då de samlat in sina data. Det skulle försämra undersökningens reliabilitet. Det är även möjligt att dessa forskare varit partiska i något avseende och systematiskt överrepresenterat de värden de försökt

mäta. (P. M. Kellstedt, G. D. Whitten, 2013). Det skulle skapa ett validitetsproblem trots att jag själv potentiellt inte gjort systematiska fel.

Därutöver kan jag naturligtvis även själv göra slarvfel. Dock tenderar slarvfel som enbart påverkar enskilda mätningar att inte vara av lika stor betydelse som systematiska fel (P. M. Kellstedt, G. D. Whitten, 2013). Med många observationer påverkas inte genomsnittsvärden speciellt mycket av slarvfel, då slumpmässiga slarvfel tenderar att ta ut varandra. Exempel på sådant jag gjort som skulle ha kunnat leda till slarvfel är bl.a. flyttande av data mellan olika SPSS-filer och felaktig namngivning av variabler. Ett annat exempel är då jag raderat fall från mitt datamaterial som enbart innehåller data från den ena, av de två enkäter som deltagarna i undersökningen svarat på. Vid sådan manipulation av data kan det ske slarvfel som påverkar reliabiliteten, eller potentiellt även validiteten hos undersökningen.

#### **4.4 Beroende variabel**

I Pew Reserchs tredje enkätundersökning ställer man deltagarna frågor gällande vem det är acceptabelt för de amerikanska myndigheterna att övervaka, t.ex. “ In your opinion, is it acceptable or unacceptable for the American government to monitor communications from citizens of other countries?” Man frågar även enkätdeltagarna om deras nivå av oro över myndigheters övervakning av olika delar av deras internetaktivitet. Dessa frågor tar fasta vid olika specifika aspekter av användning av internet eller annan elektronisk kommunikation, såsom e-mail eller användning av sökmotorer, med undantag från den första av frågorna (nr 17) som är mera allmänt formulerad. Denna fråga lyder: “Overall, how concerned are you about government surveillance of Americans’ data and electronic communications?”. Detta är den fråga jag valt för att mäta min beroende variabel. Svarande ges fyra olika svarsalternativ: 1) “Very concerned” 2) “Somewhat concerned” 3) “Not very concerned” 4) “Not at all concerned”. De är även kodade enligt denna logik i datamaterialet: 1 = “Very concerned” 2 = “Somewhat concerned” 3 = “Not very concerned” 4 = “Not at all concerned”. Jag valde att inledningsvis koda om variabeln till den raka motsatsen d.v.s. 4 = “Very concerned”, 3 = “Somewhat concerned”, 2 = “Not very concerned”, 1 = “Not at all concerned”. Det verkade mera logiskt att personer som känner mest oro ges det högsta

värde så att nivån av oro stiger tillsammans med värdet för variabeln. I mina hypoteser använder jag formuleringen “oro gällande myndigheters övervakning på internet”. Min tolkning är att högre nivå av “concern” betyder det samma som mera oro. Denna variabel är ordinal. För utförandet av min analys skapade jag en binär variabel som baserar sig på denna ordinala variabel. Jag har kodat denna genom att likställa de två högsta värdena för min beroende variabel: 4 = “Very concerned”, 3 = “Somewhat concerned” med värdet 1, där 1 = “concerned” och de två lägsta värdena för min beroende variabel: 2 = “Not very concerned”, 1 = “Not at all concerned” med värdet 0, där 0 = “not concerned”. Det medför naturligtvis vissa potentiella problem. Denna kodning skapar en förenklad form av min ursprungliga ordinala variabel. Den interna variation som finns i kategorierna för den binära variabeln uteblir och det kan leda till att skillnaden mellan personerna i de två kategorierna överdrivs. För att testa huruvida resultaten från den binära analysen är beroende av omkodning utförde jag även en ordinal regressionsanalys (se Bilagor)

För att återgå till de krav man bör uppfylla då man gör en enkätundersökning: 1) Frågan får inte vara för komplicerad. Det verkar sannolikt att de flesta som svarat inte uppfattat denna fråga som speciellt komplicerad. 2) Undvik svåra ord. “electronic communications” kan kanske uppfattas som en aning svårtolkat 3) Undvik vaga ord. Frågan innehåller inte vaga ord. Dock kan frågan i sin helhet tolkas som avsedd att vara något vag, givet att den inleds med ordet “Overall”. 4) Ställ en tillräckligt kort fråga. Verkar uppfylla detta krav. 5) Fråga en sak i taget. Frågan handlar om svarandes attityd till en enda sak, inte mera 6) Undvik negationer. Frågan innehåller inte några negationer. (Esaiasson m.fl., 2012). Vad det gäller huruvida frågan är ledande, kan det i alla fall konstateras att det inte är fråga om en samtycksfråga. Undersökningens deltagare skall uppge styrkan av en attityd, inte hålla med om eller vara emot ett enskilt påstående.

Svaret på denna fråga mäter en viktig aspekt av vilken inställning människor har till myndigheters övervakning av elektroniska kommunikation, d.v.s. nivån av oro de har gällande sådant agerande. Eftersom myndigheters övervakning av elektronisk kommunikation innebär informationsinsamling av personlig information gällande amerikanska medborgare och eftersom nivån av oro är en aspekt av deras attityd., kommer svaret på denna fråga att fungera som ett mått på vilken attityd amerikaner har till informationsinsamling av personlig information online av myndigheterna. Hur de svarande i enkätundersökningen har svarat tänker jag använda som ett mått på vilket

förhållningssätt amerikaner har till att myndigheter samlar in personlig information gällande deras internetanvändning. “Electronic communication” betyder även sådant som t.ex. telefonsamtal. Dock är de flesta exempel på elektronisk kommunikation sådan aktivitet som sker via internet.

Nedanstående tabell visar hur frekvenserna för den ursprungliga ordinala variabeln och min binära beroende variabel är fördelade mellan olika värden:

<i>Attityd till online- övervakning</i>		<i>Frekvens</i>	<i>Procent</i>	<i>Giltig procent</i>	<i>Kumulativ procent</i>
<i>Giltiga</i>	Inte alls orolig	58	9,6	12,4	12,4
	Inte speciellt orolig	152	25,0	32,5	44,9
	Ganska orolig	182	30,0	38,9	83,8
	Mycket orolig	76	12,5	16,2	100,0
	Totalt	468	77,1	100,0	
	<i>Saknas</i>	139	22,9		
<i>Totalt</i>		607	100,0		

Tabell 1 Frekvens och procentvärden för ordinal beroende variabel

<i>Binär Beroende variabel</i>		<i>Frekvens</i>	<i>Procent</i>	<i>Giltig procent</i>	<i>Kumulativ procent</i>
<i>Giltiga</i>	Inte orolig	210	34,6	44,9	44,9
	orolig	258	42,5	55,1	100,0
	Totalt	468	77,1	100,0	
<i>Saknas</i>		139	22,9		
<i>Totalt</i>		607	100,0		

Tabell 2 Frekvens och procentvärden för binär beroende variabel

I kolumnen “Giltig Procent” visas den procentuella andelen fall, av de fall som hade ett värde för denna variabel, som fick de olika värdena för denna variabel. Andelen fall som placerar sig i någon av de mittersta kategorierna d.v.s. “Not very concerned” eller “Somewhat concerned” är totalt 334 stycken vilket är 70,3 %

En klar majoritet undviker alltså ytterlighetspositionerna gällande hur oroliga de känner sig i förhållande till övervakning online. Då jag programmerat om denna ordinala variabel till en binär variabel kan det medföra vissa problem. Den verkliga skillnaden mellan åsikterna hos en person jag kategoriserar som “orolig” och en person som kategoriseras som “inte orolig”, kan i många fall vara förhållandevis liten. Det försämrar validiteten hos detta mått. Dock återstår ca 30 % som intar en tydlig ståndpunkt och dessa personer finns förstås representerade inom båda kategorierna hos den binära variabeln. Eftersom en klar andel (70 %) placerar sig inom de två mittersta kategorierna, verkar det trots allt vara motiverat att behandla denna beroende variabel som en binär variabel.

## 4.5 Oberoende variabler

Min första oberoende variabel är ålder, vilket alla deltagare i enkätundersökningen blivit frågade om då de valt att delta. Svarsalternativen för ålder är positiva heltal. Samma gäller min andra oberoende variabler som är kön. I mitt datamaterial är 1 = man och 2 = kvinna. Jag kommer att analysera kön som en nominal variabel. Den tredje oberoende variabeln i min undersökning är utbildningsgrad. Denna variabel planerar jag att mäta med det alternativ respondenterna har angett gällande sin utbildningsnivå: 1) less than high school 2) High school 3) Some college 4) Bachelors degree or higher.

Min fjärde oberoende variabel är institutionellt förtroende vilket jag tänker mäta med svaret på frågan Pew Research ställde enkätundersökningens deltagare i den första enkäten: How much of the time do you think you can trust the **government** in Washington to do what is right? Svarsalternativen är: 4) Just about always 3) Most of the time 2) Only some of the time 1) Never. Om man litar på att staten gör det rätta “just about always”, kan man alltså anses ha ett högt förtroende för statsmakten, medan “never” innebär ett lågt förtroende eller till och med avsaknaden av förtroende. Utgående ifrån de olika krav man kan ställa på en välformulerad fråga, som jag gick igenom tidigare i detta kapitel, verkar det inte finnas några tydliga problem med denna fråga. Frågan avslutas med uttrycket “to do what is right”, vilket kanske kan anses vara en aning mångtydigt, men i övrigt är frågan tydligt formulerad, opartisk (icke-ledande) och tillräckligt simpel och svarsalternativen är uttömmande och ömsesidigt uteslutande.

Min tredje hypotes är: **Högre förtroende för myndigheter har ett negativt samband till en individs oro gällande myndigheters övervakning på internet.** De som svarat “Just about always” eller “Most of the time” borde alltså generellt sätt uttrycka mindre oro i förhållande till statens övervakning av amerikaners data och elektroniska kommunikation än de som svarat “Only some of the time” eller “Never”, givet att hypotesen är korrekt.

Min femte oberoende variabel är graden av politisk avvikelse. I den tredje enkäten ställer man följande frågor: “In general, would you describe your political views as... very conservative, conservative, moderate, liberal, very liberal? Den här frågan ger en viss inblick i var någon placerar sig politiskt. Dock blir denna inblick rätt så begränsad. Att undersökningens deltagare själva väljer sin position kan medföra vissa reliabilitetsproblem eftersom olika personer kan tolka vad det innebär att vara t.ex. konservativ på olika sätt. Oberoende av hur man gör en sådan tolkning är dock avvikande från den politiska mitten det samma och det är just den aspekten av människors politiska positionering jag är intresserad av. Jag kommer att räkna de som antingen säger att de är “very liberal” eller “very conservative” som politiskt avvikande. En person som ger ett sådant svar positionerar sig själv längre från den politiska mitten och anser således själv att hen avviker i något avseende. Den ursprungliga kodningen för variabeln var sådan att “very liberal” = 1 och de andra värdena var kodade i stigande ordning till 5 så att “very conservative” = 5. Jag kodade om variabeln så att “very liberal” och “very conservative” båda är 2, emedan “liberal” och “conservative” båda är 1 samt moderate = 0. På det sättet får respondenterna ett högre värde desto längre från den politiska mitten de positionerar sig, vilket passar syftet jag har med denna variabel d.v.s. att mäta politisk avvikelse.

Man frågar även “From what you know, do you agree or disagree with the Tea Party movement, or don’t you have an opinion either way?”. Här tänker jag mig att en person som svarar “agree” tar avstånd från den politiska mitten. Denna frågas koppling till politisk avvikelse kanske inte är så tydligt som vore önskvärt, men det kan trots det vara intressant att se vilket samband som finns mellan svaren på frågan och den beroende variabeln. Jag behandlar svaret på denna fråga som en separat variabel med koppling till politisk avvikelse. Min fjärde hypotes är: **Det finns ett positivt samband mellan hur politiskt avvikande någon är och denna individs oro gällande myndigheters övervakning på internet.** Personer som svarar “very liberal” eller “very conservative”



borde alltså generellt sätt uttrycka mera oro i förhållande till statens övervakning av amerikaners data och elektroniska kommunikation för att denna hypotes skall kunna verifieras. Jag tänker mig dessutom att personer som svarar "agree" gällande huruvida de understöder Tea Party rörelsen, kommer att uttrycka större oro.

Min sjätte oberoende variabel är: Kännedom om statlig elektronisk övervakning med syfte att motverka terrorism. Vad som menas är hur mycket någon har hört om sådan statlig verksamhet. Det handlar alltså inte om hur mycket någon känner till om statlig elektronisk övervakning i allmänhet, utan sådan övervakning som uttryckligen utförs med den officiella motiveringen att övervaka terrorismrelaterad aktivitet. Jag kommer att mäta denna variabel med svaret på fråga 17 i den första enkäten av Pew Research: How much, if anything, have you heard about the government collecting information about telephone calls, emails and other online communications as part of efforts to monitor terrorist activity? Have you heard...Svarsalternativen är: 1) "A lot", 2) "A little", 3) "Nothing at all", 4 "Don't know". Det är alltså fråga om en variabel på ordinalnivå. I min analys har jag kodat om variabeln så att 1 = "Nothing at all", 3 = "A lot", medan 2 har samma värde. Den hypotes som relaterar till denna variabel lyder: **Kännedom om statlig elektronisk övervakning med syfte att motverka terrorism har en negativ effekt på en individs oro gällande myndigheters övervakning på internet.** För att hypotesen skall stämma krävs det därmed att personer med ett högre värde på denna oberoende variabel tenderar att ha ett lägre värde på den beroende variabeln, alltså lägre oro i förhållande till statlig övervakning online.

Sammantaget har jag alltså fem stycken ordinala oberoende variabler: utbildningsnivå, politisk avvikelse, institutionellt förtroende och kännedom om statlig elektronisk övervakning med syfte att motverka terrorism samt attityd till Tea Party rörelsen. Dessa variabler är ordinala därför att deras värden består av kategoriska svarsalternativ som kan rangordnas. Därutöver har jag en kontinuerlig variabel: ålder, och en nominal variabel: kön.

Nedanstående tabell visar frekvenser för de oberoende variablerna i min analys d.v.s. hur vanliga olika svarsalternativ har varit bland respondenterna då de svarat på de frågor som jag använder för att mäta mina variabler. Tabellen visar även frekvensen för värden för ålder och kön. Frekvenstabellen för ålder baserar sig på en uppdelning av variabelns värden i 6 kategorier för att skapa överskådlighet.

<i>Ålder, kategorisk</i>		<i>Frekvens</i>	<i>Procent</i>	<i>Giltig procent</i>	<i>Kumulativ procent</i>
<i>Giltiga</i>	Under 30	76	12,5	17,7	17,7
	30-40	84	13,8	19,5	37,2
	40-50	85	14,0	19,8	57,0
	50-60	96	15,8	22,3	79,3
	60-70	84	13,8	19,5	98,8
	Över 70	5	,8	1,2	100,0
	Totalt	430	70,8	100,0	
<i>Saknas</i>		177	29,2		
<i>Totalt</i>		607	100,0		

Tabell 3 Frekvens och procentvärden för ålder (kategorisk)

Uppdelningen mellan de ålderskategorierna är rätt så balanserad med undantag för personer över 70 som bara innehåller 5 personer.

<i>Kön</i>		<i>Frekvens</i>	<i>Procent</i>	<i>Giltig procent</i>	<i>Kumulativ procent</i>
<i>Giltiga</i>	Man	241	39,7	50,7	50,7
	Kvinna	234	38,6	49,3	100,0
	Totalt	475	78,3	100,0	
<i>Saknas</i>		132	21,7		
<i>Totalt</i>		607	100,0		

Tabell 4 Frekvens och procentvärden för kön

Av de fall som inte saknar värden är den procentuella andelen män och kvinnor nära en 50/50 uppdelning. Detta förhållande är naturligtvis nära det verkliga procentuella förhållandet i populationen, vilket är betydelsefullt för att resultatet skall ha validitet. Då jag t.ex. ser på andelen personer som säger sig vara mycket oroliga gällande statlig online övervakning, kan denna andel avvika från det verkliga värdet i populationen ifall deltagarna i enkäten har en annan könsfördelning än populationen och ifall kön har ett samband till denna attityd.

<i>Politisk avvikelse</i>		<i>Frekvens</i>	<i>Procent</i>	<i>Giltig procent</i>	<i>Kumulativ procent</i>
<i>Giltiga</i>	centerposition	207	34,1	44,7	44,7
	Avviker lite från center	193	31,8	41,7	86,4
	Avviker från center	63	10,4	13,6	100,0
	Totalt	463	76,3	100,0	
<i>Saknas</i>		144	23,7		
<i>Totalt</i>		607	100,0		

Tabell 5 Frekvens och procentvärden för politisk avvikelse

De flesta personer som deltagit i undersökningen positionerar inte sig själva långt från mitten på en politisk vänster-högerskala. Av de giltiga fallen, är den procentuella andel som klart avviker i detta avseende 13 %. Med andra ord tar lite mindre en var sjunde person politiskt sätt klart avstånd från den politiska centern.

<i>Tea Party</i>		<i>Frekvens</i>	<i>Procent</i>	<i>Giltig procent</i>	<i>Kumulativ procent</i>
<i>Giltiga</i>	Understöder	63	10,4	13,7	13,7
	Understöder inte	162	26,7	35,1	48,8
	Ingen åsikt	236	38,9	51,2	100,0
	Totalt	461	75,9	100,0	
<i>Saknas</i>		146	24,1		
<i>Totalt</i>		607	100,0		

Tabell 6 Frekvens och procentvärden för Tea Party understöd

Kring 13 % av respondenterna säger sig understöda Tea Party rörelsen. Denna andel är alltså ungefär samma som andelen personer som svarat ”very conservative” eller ”very liberal” och således räknas som klart avvikande från den politiska centern.

<i>Institutionellt förtroende</i>		<i>Frekvens</i>	<i>Procent</i>	<i>Giltig procent</i>	<i>Kumulativ procent</i>
<i>Giltiga</i>	Aldrig	68	11,2	14,5	14,5
	Ibland	319	52,6	67,9	82,3
	För det mesta	76	12,5	16,2	98,5
	Nästan alltid	7	1,2	1,5	100,0
	Totalt	417	77,4	100,0	
<i>Saknas</i>		137	22,6		
<i>Totalt</i>		607	100,0		

Tabell 7 Frekvens och procentvärden för institutionellt förtroende

Det klart vanligaste värdet institutionellt förtroende antar är: enbart en del av tiden (“Only some of the time”), där hela 67.9 % placerade sig i denna kategori. Förtroendet för de amerikanska myndigheterna är inte speciellt högt, men de flesta skulle ändå inte gå så långt som att svara aldrig, gällande hur ofta de har förtroende för politiska institutioner.

<i>Kännedom om statlig övervakning med syfte att motverka terrorism</i>		<i>Frekvens</i>	<i>Procent</i>	<i>Giltig procent</i>	<i>Kumulativ procent</i>
<i>Giltiga</i>	Inget alls	27	4,4	6,1	6,1
	Lite	210	34,6	47,2	53,3
	Mycket	208	34,3	46,7	100,0
	Totalt	445	73,3	100,0	
<i>Saknas</i>		162	26,7		
<i>Totalt</i>		607	100,0		

Tabell 8 Frekvens och procentvärden för kännedom om statlig övervakning med syfte att motverka terrorism

De allra flesta som svarat har hört mera än ingenting om övervakning med syfte att motverka terrorism. Bara 6 % procent säger sig inte ha hört något. Detta är kanske inte så överraskande då det varit ett omdiskuterat ämne i USA, framfört allt direkt efter Edward Snowdens informationsläckande, vilket är tidpunkten för datainsamlingen.

<i>Utbildning</i>		<i>Frekvens</i>	<i>Procent</i>	<i>Giltig procent</i>	<i>Kumulativ procent</i>
<i>Giltiga</i>	Mindre än gymnasie-utbildning	54	8,9	11,4	11,4
	Gymnasie-utbildning	133	21,9	28,0	39,4
	Lite universitets-utbildning	123	20,3	25,9	65,3
	Kandidat examen eller högre	165	27,2	34,7	100,0
	Totalt	475	78,3	100,0	
<i>Saknas</i>		132	21,7		
<i>Totalt</i>		607	100,0		

Tabell 9 Frekvens och procentvärden för utbildning

Olika utbildningsnivåer är rätt så jämnt representerade bland respondenterna. Undantaget är personer med lägre utbildning än gymnasieutbildning som bildar en lägre procent.

## 4.6 Kausalitet

Mitt data härstammar alltså från en enkätundersökning och denna undersökning är en observationsstudie av typen tvärsnittsstudie. Att det är frågan om en tvärsnittsstudie bestäms av det faktum att jag undersöker flera olika spatiala enheter vid en viss tidpunkt. De spatiala enheter jag undersöker är förstås individer, alltså amerikanska medborgare. Eftersom den undersökning varifrån jag hämtat mitt data inte utförts som ett experiment, där man manipulerat de oberoende variabelernas värden, är variationen hos mina oberoende variabler alltså inte ett resultat av slumpmässig tilldelning av undersökningens forskare. Man har istället studerat amerikaners attityder och socio-ekonomiska karaktärsdrag sådana som de är. Det är vad som menas med att det är en observationsstudie. (P. M. Kellstedt, G. D Whitten, 2013)

Att det är frågan om just en observationsstudie och inte ett kontrollerat experiment medför vissa utmaningar i att dra tillförlitliga slutsatser, då man analysera ifrågavarande data. En utmaning handlar om i vilken utsträckning andra möjliga förklarande faktorer,

som även samvarierar med de oberoende variablerna, kan uteslutas, så att den effekt de oberoende variablerna har på min beroende variabel kan isoleras. Om det inte förekommer någon samvariation mellan mina oberoende och min beroende variabel, krävs det även att man kontrollerar för sådana faktorer för att kunna utesluta att avsaknaden av samvariation inte är en konsekvens av deras inverkan.. I min analys kommer jag att använda mig av vissa kontrollvariabler för att minska risken för att ett sådant skensamband uppstår. Dessa variabler är kön, ålder och utbildning. Min analys kommer alltså att utreda huruvida det finns ett samband mellan min beroende variabel och mina oberoende variabler som är oberoende av dessa tre faktorer. Som exempel: Om man antar att ålder har ett positivt kausalt samband med institutionellt förtroende och även ett positivt kausalt samband med hur positivt inställd någon är till övervakning online, kan det leda till samvariation mellan institutionellt förtroende och attityd till integritet online hos enkätdeltagarna utan att det finns något kausal samband mellan dessa faktorer.

Genom att använda mig av kontrollvariabler kan jag minska risken att de samband jag eventuellt finner genom analysen, mellan mina förklarande faktorer och den variabel som skall förklaras, beror på någon tredje faktors samband med bådadera. (P. M. Kellstedt, G. D Whitten, 2013). Hur det data jag använder mig av har samlats in, har alltså en betydelse för hur jag måste gå till väga då jag analyserar det. Därför är det nödvändigt att vissa delar av mitt data mäter sådana bakgrundsfaktorer som potentiellt kan ge upphov till "false positivs" i min analys. Jag kommer alltså att se på den påverkan som vissa faktorer potentiellt har på människors attityd till integritet på internet. Detta handlar om ett kausalt påstående. Jag påstår att vissa egenskaper hos människor, så som t.ex. deras förtroende för statliga institutioner, påverkar deras inställning till att myndigheterna samlar in data gällande deras onlineaktivitet. Paul M. Kellstedt och Guy D. Whitten ställer upp fyra kriterier för kausala relationer: 1) "Is there a credible causal mechanism that connects X to Y " 2) "Can we rule out the possibility that Y could cause X? " 3) "Is there covariation between X and Y? "4) "Have we controlled for all confounding variables Z that might make the association between X and Y spurious? ". För att besvara dessa frågor i ordning: 1) Jag behandlar denna fråga i kapitel 6 där jag motiverar mina hypoteser. Kortfattat så tänker jag mig att människor som har mindre förtroende för myndigheterna anser att risken är högre att den information myndigheterna samlar in om privatpersoner används på ett sätt som

skadar dem, vilket gör dem mindre villiga att understöda sådan informationsinsamling. Vad det gäller politisk avvikelse handlar den kausala mekanism jag anser förklara ett potentiellt samband, om hur personer som bryter mot det som är normativt, har ett större behov av privatliv för att undvika negativa sociala påföljder, vilket även gäller brott mot det som är politisk normativt. Den kausala mekanismen som kopplar ihop kännedom om statlig övervakning med syfte att motverka terrorism och attityd till övervakning online, är hur personer som hör mera om hur staten utför sådan övervakning, kan tänkas koppla ihop terroristbekämpning och onlineövervakning i en högre utsträckning och därmed se sådan övervakning som mera motiverad. Därmed skulle dessa individer kunna tänkas ha en mera positiv, tolerant attityd till statlig övervakning online.

2) Den mätning som gjorts av attityd till informationsinsamling online av amerikanska myndigheter, d.v.s. vad jag använder för att mäta min beroende variabel, föregår mätningen av mina oberoende variabler tidsmässigt. Det är ingen garanti för att den kausala relationen inte har omvänd tidsordning, men för att det skall kunna vara frågan om en orsak-verkan relation, måste orsaken föregå verkan.

3) Jag kommer att utföra en statistisk analys för att avgöra om variablerna samvarierar.

4) Jag kommer knappast nära kontrollerandet av alla sådana variabler som kan skapa samvariation utan att det finns en verkligt kausalt relation, men jag kommer att använda vissa kontrollvariabler så som kön, ålder och utbildning för att minska risken att detta sker.

Eftersom det inte är ett experiment är det inte genom slumpen som det avgörs vem som har vilken nivå av institutionellt förtroende eller politisk avvikelse (P. M. Kellstedt, G. D Whitten, 2013, s.74). Därmed kan det, som jag redan gått in på, finnas en egenskap hos de personer som t.ex. har lågt förtroende som även ger dem låg tolerans för myndigheters övervakning online d.v.s. en egenskap som leder till både lågt förtroende och låg tolerans. Detta är en viktig risk, som jag dels måste försöka minska då jag utför min statistiska analys med hjälp av kontrollvariabler, dels något jag måste uppmärksamma då jag drar slutsatser gällande min undersöknings resultat.

## 4.7 Generalisering

Vad det gäller generalisering av de resultat jag får av min analys skulle det förstås vara intressant att veta huruvida människor i andra länder även följer ett liknande mönster i sitt förhållningssätt till integritet online som amerikaner. Dock är det amerikanska samhället möjligtvis avvikande andra länder i sådana avseenden som påverkar resultatet. Detta är relaterat till validitet (Landman, 2003). Ett exempel skulle vara att jag skulle göra samma analys med data gällande ett annat land, t.ex. Finland, där enkättagarna skulle frågas vad de tänker om statlig övervakning online. Det skulle inte utan vidare kunna jämföras med den amerikanska enkätundersökning jag i praktiken använder mig av.

De finska myndigheternas övervakning på internet och den amerikanska statens övervakning är olika saker, inte enbart i termer av geografi, vilket respondenterna i respektive undersökning högst sannolikt är medvetna om. Även om jag alltså skulle kunna utföra samma analys, skulle vad jag mera specifikt undersöker kunna variera mellan olika länder, vilket jag skulle vara tvungen att hålla i tankarna då jag jämför resultatet från dessa två analyser. Om frågorna i enkäten hade varit formulerade på ett sådant sätt att de tar fasta vid sådant statligt agerande generellt sätt, t.ex. "Vad tycker du om att stater samlar in information online om sina medborgare?", skulle det kanske ha varit lättare att generalisera resultatet till andra länder. Dock var frågorna inte formulerade på ett sådant sätt utan de refererade till den amerikanska statens övervakning, som säkerligen har sina särdrag. De amerikaner som deltog i undersökningen tog ställning till en statsmakt som bl.a. inkluderar NSA och vars rykte, både i USA och utomlands, skiljer från andra stater gällande övervakning. Den undersökning jag utför gäller ett fenomen som inte egentligen finns i andra länder. Frågor som använder generella begrepp skulle dock fortfarande kunna producera vissa problem, eftersom människor i olika länder kan tänkas tolka vissa ord på ett varierande sätt.

Möjligheten att generalisera påverkas alltså av huruvida de fenomen man undersöker har en varierande betydelse i olika sammanhang. Om en sådan variation förekommer innebär det att undersökningens externa validitet minskar (Landman, 2003). Om min undersökning t.ex. visar att amerikaner som har högre institutionellt förtroende har en mera negativ attityd till att myndigheterna samlar in information om dem, kan den



varierande innebörden som ges myndigheters informationsinsamling och institutionellt förtroende i olika länder göra det problematiskt att generalisera.

## 4.8 Statistisk Metod

För att analysera det statistiska förhållandet mellan mina variabler kommer jag att använda mig av binär logistisk regressionsanalys. Orsaken till att jag använder denna typ av analys är till att börja med, att min beroende variabel är kvalitativ. Då amerikaner svarat på Pew Researchs enkätundersökning gällande sin inställning till myndigheters övervakning av deras elektroniska kommunikation, har de haft fyra olika svarsalternativ att välja mellan. Dessa fyra alternativ kan rangordnas men trots det är avståndet mellan dem inte något som går att avgöra. De kan dock delas in i höga och låga värden, alltså människor som är oroliga i förhållande till statlig övervakning online och de som inte är det, vilket i sin tur skapat min binära beroende variabel. Därmed en binär regressionsanalys.

Ett av alternativen då man utför en regressionsanalys är att utföra en linjär regressionsanalys. Utfallet av en sådan analys ger funktionen för den linje som beskriver sambandet mellan variablerna så väl som möjligt. Eftersom min beroende variabel kan anta två olika värden, skulle mitt data i en graf med den beroende variabeln på y-axeln och en oberoende variabel på x-axeln skapa ett mönster med punkter på två olika nivåer, likt två parallella linjer. Om man beskriver ett sådant datamaterial med en linjär funktion kommer den linje som utgör funktionens graf, vid tillräckligt höga eller låga värden på den oberoende variabeln, att anta sådana värden på den beroende variabeln, som denna inte kan anta (F. C. Pampel, 2011). En linjär regressionsanalys beskriver ett kontinuerligt förhållande mellan variablerna, medan den beroende variabeln enbart kan anta vissa diskreta värden.

För en binär variabel kommer genomsnittsvärdet på den beroende variabeln, för fall med ett visst värde på den oberoende variabeln, att ge sannolikheten för att ett godtyckligt fall får värdet 1 på den beroende variabeln (F. C. Pampel, 2011). Då man anpassar en linje till ett sådant datamaterial kommer vissa värden på den oberoende variabeln att ge värden som är under 0 eller över 1, vilket går utanför de värden som

kan ges en meningsfull tolkning, eftersom sannolikheten för att någonting inträffar måste ligga mellan 0 och 100 procent (Bjerling, 2010).

Ett annat problem som uppstår då man utför en linjär regressionsanalys för att analysera en kategorisk variabel har att göra med ett antagande som linjära regressionsanalyser baserar sig på, som på engelska heter *the assumption of additivity*. Detta antagande innebär att effekten en variabel har på den beroende variabeln är lika stor, oberoende av vilket värde andra oberoende variabler har. Detta antagande uppfylls inte för vissa variabelvärden då den beroende variabeln är kategorisk. Om en annan oberoende variabel har ett högt värde som påverkar sannolikheten för att den beroende variabeln får ett visst utfall, så att denna sannolikhet ligger nära 1 eller 0, kommer effekten av en höjning av den ifrågavarande oberoende variabeln på denna sannolikhet att minska (F. C. Pampel, 2011). Det leder till att förhållandet mellan den oberoende variabeln och den beroende variabeln inte längre är linjärt, då en höjning av den oberoende variabelns värde med en enhet leder till en allt mindre förändring av sannolikheten för att den beroende variabelns värde skall vara 1, desto närmare denna sannolikhet kommer 0 eller 1. Dessa problem gör en linjär regressionsanalys till ett bristfälligt alternativ för att analysera en modell med en kategorisk beroende variabel.

Som en lösning på dessa problem kan man, istället för att analysera förhållandet mellan oberoende variabler och sannolikhet för att ett fall skall placera sig inom en viss kategori på den beroende variabeln, analysera förhållandet mellan oberoende variabler och den naturliga logaritmen för oddsen, eller de loggade oddsen, för att så skall ske. Eftersom den effekt som en förändring av sannolikheten för ett visst utfall har på detta logaritmiska värde ökar, desto närmare sannolikhetsvärdet kommer 0 eller 1, kan förhållandet beskrivas linjärt (F. C. Pampel, 2011). Fördelen är att detta förhållande kan beskrivas på ett mycket enklare sätt än det icke-linjära förhållande som analysen av sannolikhetsvärden för den beroende variabeln skulle se på. Kravet om additivitet uppfylls eftersom en förändring av en oberoende variabels värde ger samma förändring av de loggade oddsen, oberoende av vilket värde andra oberoende variabler har (F. C. Pampel, 2011).

Denna sorts analys kallas för en logistisk regressionsanalys, vilket är den analys jag kommer att använda mig av. Då man tolkar koefficienten för utfallet av denna analys, kan det göras på ett, i princip, likadant sätt som för en linjär regressionsanalys. Denna

koefficient anger hur mycket värdet på y-axeln ändrar givet en enhetsförändring av värdet på x-axeln. Skillnaden ligger i att y-axeln i denna analys mäter de loggade oddsen för att den beroende variabeln skall få ett visst utfall (Bjerling, 2010). Det som återstår att göra är alltså att tolka vad en förändring av de loggade oddsen innebär för oddsen och sannolikheten för att den beroende variabeln får värdet 1.

Nackdelen med de loggade oddsen som värde är att de inte säger något speciellt tydligt om hur sannolikheten för den beroende variabeln påverkas av en oberoende variabel (F. C. Pampel, 2011). Om du t.ex. vet att en enhetshöjning av en oberoende variabel leder till att de loggade oddsen stiger med 0.8, är det inte uppenbart hur detta relaterar till huruvida den beroende variabeln kommer att vara 1 eller 0, givet denna förändring av den oberoende variabelns värde. Vad man kan göra för att göra detta resultat mera lättolkat, är att räkna om förändringen av de loggade oddsen till den procentuella förändringen av oddsen för ett visst utfall. Om man t.ex. känner till koefficienten för den linjära funktion som beskriver förhållandet mellan de loggade oddsen för sannolikheten att en person säger sig vara orolig gällande statlig övervakning av elektronisk kommunikation och institutionellt förtroende, kan man beräkna hur oddsen för att en person placerar sig i kategorin "orolig" förändras procentuellt då graden av institutionellt förtroende ökar med en enhet.

Vad som menas med odds är sannolikheten att en händelse inträffar dividerat med sannolikheten att denna händelse inte inträffar. För att beräkna den procentuella förändringen av oddsen, givet en enhetsökning av den oberoende variabeln, räknar man ut vad Eulers tal(ca 2,71828), som är konstanten som är bas i den naturliga logaritmen, upphöjt till de loggade oddsen blir. Sedan tar man detta resultat -1 och gånger 100, eftersom det värde man får av den första uträkningen ökar oddsens värde i den mån det överstiger 1. Då man multiplicerar med hundra omvandlar man från decimalform till procent. (F. C. Pampel, 2011)

Denna ökning av oddsen är ett något mera lättolkat värde. Dock är det viktigt att komma ihåg att odds inte är det samma som sannolikhet. Eftersom förhållandet mellan den oberoende variabeln och sannolikheten för ett visst utfall för den beroende variabeln inte är linjärt, kan förhållandet mellan variablerna inte beskrivas med en simpel linjär funktion och dess koefficient. Detta var det problem som användandet av logistisk regressionsanalys var till för att lösa.

Det man dock kan göra, är att beräkna sannolikhetsvärden för utfall för den beroende variabeln vid enskilda värden på en oberoende variabel. En grafiska framställning av dessa uträkningar visar hur de oberoende variablerna hänger ihop med den beroende variabeln på ett intuitivt sätt. I min statistiska analys har jag, utöver en binär logistisk regressionsanalys, även utfört en ordinal logistisk regressionsanalys (se Bilagor s. 76). För att återgå till att diskutera undersökningens validitet, borde min binära analys ha validitet så länge det samband som den potentiellt visar, även syns i den ordinala analysen. Det skulle demonstrera att sambandet inte är en konsekvens av hur jag kodat om min beroende variabel. I nästa kapitel finns grafer för sambandet mellan de olika oberoende variablerna och sannolikhetsvärden för att min binära beroende variabel skall få värdet 1.

Då jag gjort min binära logistiska regressionsanalys har jag behandlat mina ordinala oberoende variabler samt ålder som kontinuerliga variabler, som i SPSS kallas "covariate", och kön som en binär variabel, vilket går under benämningen "factors".

En annan sak, utöver ovannämnda värden för sambandet mellan variablerna, som utfallet av en sådan analys visar, då man utför denna i ett statistikprogram såsom SPSS som jag har gjort, är hur hög signifikansnivå för de olika värden man fått är. Så som jag diskuterat tidigare i detta kapitel, är antalet fall avgörande för detta värde och den relativa andelen fall i förhållande till den totala populationens storlek är i regel av liten betydelse. Därmed kan statistikprogrammet räkna ut vilken signifikansnivå resultatet har. I nästa kapitel skall jag gå igenom det resultat jag fått i SPSS då jag genomfört min analys.

## 5. Resultat

### 5.1 Bivariat analys

Det första steget i analysen är en bivariat analys av de oberoende variablerna och den beroende variabeln. Denna analys visar vilket det statistiska förhållandet är mellan enskilda oberoende variabler och den beroende variabeln. B-värdet är koefficienten för de loggade oddsen för den binära beroende variabeln. Detta värde indikerar förändringen av sannolikheten för att den beroende variabeln har värdet 1, vid en enhetsförändring av den oberoende variabel.

		<i>B</i>	<i>Sig.</i>	<i>Exp(B)</i>
<i>Steg 1<sup>a</sup></i>	Institutionellt förtroende	-,402	,011	,669
	Konstant	1,028	,002	2,796

Tabell 10 Resultat av bivariat analys för institutionellt förtroende

Institutionellt förtroende har ett negativt B-värde vilket tyder på ett negativt samband mellan institutionellt förtroende och sannolikheten att säga sig vara orolig i förhållande till statens övervakning online. Resultatets signifikansvärde är tillräckligt högt, det är 0,011.

		<i>B</i>	<i>Sig.</i>	<i>Exp(B)</i>
<i>Steg 1<sup>a</sup></i>	Kännedom om statlig övervakning med syfte att motverka terrorism	,624	,000	1,867
	Konstant	-1,266	,002	0,282

Tabell 11 Resultat av bivariat analys för kännedom om statlig övervakning med syfte att motverka terrorism

Kännedom om statlig övervakning med syfte att motverka terrorism, d.v.s. hur mycket respondenterna hört om övervakning online med syfte att motverka terrorism, har ett

positivt samband till sannolikheten att säga sig vara orolig. Detta värde är även signifikant.

		<i>B</i>	<i>Sig.</i>	<i>Exp(B)</i>
<i>Steg 1<sup>a</sup></i>	Politisk avvikelse	,263	,054	1,300
	Konstant	,026	,844	1,026

Tabell 12 Resultat av bivariat analys för politisk avvikelse

		<i>B</i>	<i>Sig.</i>	<i>Exp(B)</i>
<i>Steg 1<sup>a</sup></i>	Tea party understöd	-,286	,033	,751
	Konstant	,886	,008	2,426

Tabell 13 Resultat av bivariat analys för Tea Party understöd

Politisk avvikelse har ett positivt samband till den beroende variabeln, medan understöd för Tea party rörelsen har ett negativt samband. Dock når inte signifikans- värdet för politiska avvikelse riktigt 5 % -nivån, då signifikansvärdet är 0,054. Signifikansvärdet för understöd för Tea party rörelsen är tillräckligt, på 0,033. På basis av denna bivariata analys är det enbart institutionellt förtroende som tillförlitligt uppvisar det samband jag förväntade mig utgående ifrån hypoteserna. Resultatet för “Politisk avvikelse” följer även förväntningarna, dock utan lika stor tillförlitlighet. Kännedom om statlig övervakning med syfte att motverka terrorism har ett positivt samband till den beroende variabeln, till skillnad från det negativa samband som förväntades. Understöd för Tea party rörelsen uppvisar ett negativt samband, då ett positivt samband förväntades. Till näst behandlas resultatet av en multivariat binär logistisk regressionsanalys, som inkluderar samtliga variabler, d.v.s. de oberoende variabler som behandlades i ovanstående bivariata analyser, kontrollvariablerna kön, ålder och utbildningsnivå, samt den beroende variabeln.

## 5.2 Binär logistisk regressionsanalys

Nedanstående tabell visar hur “kön” och “Tea party understöd” är kodade för regressionsanalysen.

<i>Kodning för kategoriska variabler</i>		<i>Frekvens</i>	<i>Parameterkodning</i>
<i>Tea Party</i>	Understöder	63	1
	Understöder inte	158	2
	Ingen åsikt	210	0
<i>Kön</i>	Man	222	1
	Kvinna	209	0

Tabell 14 Kodning av variablerna Tea party understöd och kön

B-värdet i tabell 15 i den första kolumnen är koefficienten för de loggade oddsen för den binära beroende variabeln. Det är alltså ett värde som baserar sig på förändringen av sannolikhetsvärdet för den beroende variabeln vid en enhetsförändring av en oberoende variabel, medan de andra oberoende variabelernas värden hålls konstanta. Det handlar om sannolikheten för att den beroende variabeln skall ha värdet 1, d.v.s. att en person kan kategoriseras som orolig i förhållande till statlig övervakning online.

		<b>B</b>	<b>EXP(B)</b>	<b>SIG.</b>
OBEROENDE VARIABLER	Ålder	-,004	,996	,479
	Politisk avvikelse	,104	1,109	,495
	Institutionellt förtroende	-,369	,692	,036
	Kännedom om statlig övervakning med syfte att motverka terrorism	,684	1,982	,000
	Tea Party			,162
	Tea Party(1)	,503	1,654	,130
	Tea Party(2)	-,136	,873	0,559
KONTROLL VARIABLER	Konstant	-,403	,668	,526
	Kön	-,493	,611	,020
	Utbildning	,044	1,044	,679

Tabell 15 Resultat av multivariat analys

De signifikanta B-värdena i utfallet för analysen är värdena för kön, institutionellt förtroende och kännedom om statlig övervakning med syfte att motverka terrorism. Utfallet av analysen visar att graden av kännedom om statlig övervakning med syfte att motverka terrorism har ett positivt samband till den beroende variabeln. Personer som har mera kännedom om statlig övervakning med syfte att motverka terrorism tenderar alltså att uttrycka större oro. Utfallet visar även ett negativt samband mellan institutionellt förtroende och graden av oro. Eftersom min beroende variabel baserar sig på en ordinal variabel som jag kodat om till en binär variabel, gjorde jag även en ordinal logistisk regressionsanalys för att bekräfta att de resultat jag når gällande variabelernas samband är giltigt oberoende av omkodningen.

Denna ordinala analys bekräftar förekomsten av de samband som visas i den binära analysen med undantag för resultatet gällande kön. Det demonstrerar att de övriga sambanden existerar oberoende av den nya kodning som den beroende variabeln fick, då den binära variabeln skapades. Att vara man innebär, på basis av den binära analysen, att sannolikheten är lägre för att vara orolig i förhållande till statlig övervakning online, då koefficienten för de loggade oddsen är -0,493. I den ordinala analysen uppvisades även ett negativt samband mellan att vara man och den beroende variabeln, dock var detta värde inte statistiskt signifikant.

Sammanfattningsvis bekräftar denna multivariata binära regressionsanalys det resultat som den bivariata analysen visade, d.v.s. att "Kännedom om statlig övervakning med syfte att motverka terrorism" har ett positivt samband och institutionellt förtroende har ett negativt samband till den beroende variabeln.

### **5.3 Prediktiv sannolikhet för binär beroende variabel**

Nedanstående grafer visar förhållandet mellan mina oberoende variabler och den predicerade sannolikheten för att den binära beroende variabeln skall ha värdet 1, d.v.s. hur sannolikt det är för olika värden på de oberoende variablerna att en person är orolig i förhållande till myndigheters övervakning online. Det är sammanlagt 10st grafer och varje graf har en x-axel som representerar värden på en enskild oberoende variabel och en y-axel som representerar den predicerade sannolikhet för den binära beroende



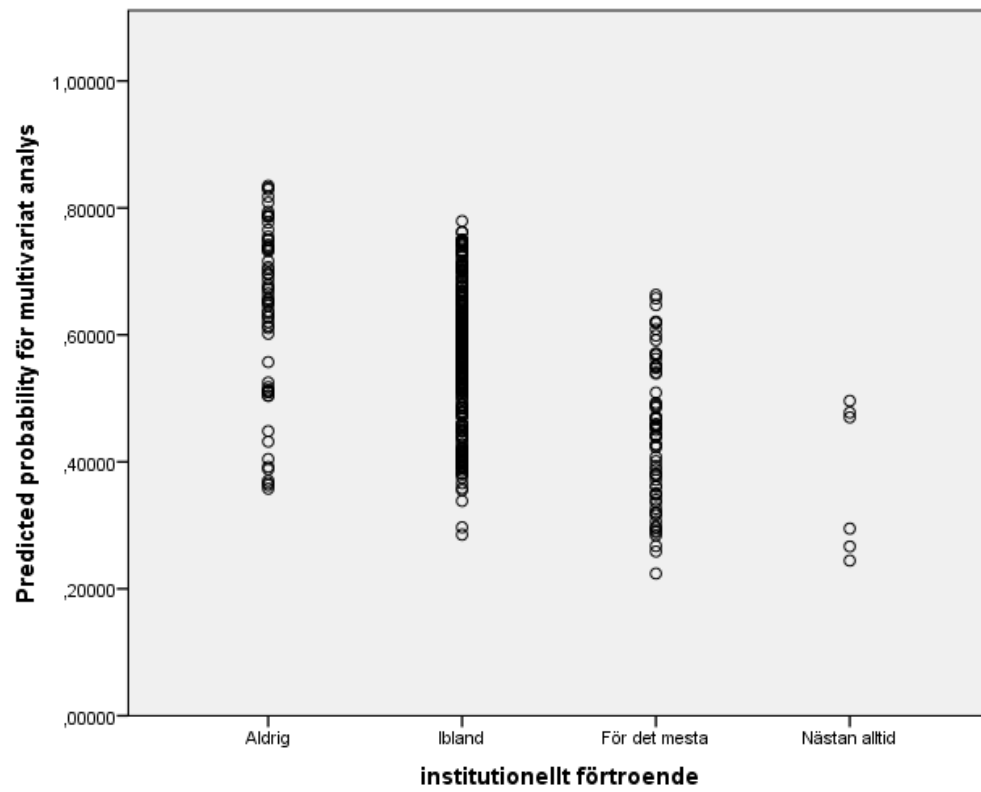
variabeln. De många olika punkterna för ett visst x-värde i de grafer som inkluderar samtliga värden beror av de andra oberoende variabelnas värden. I den mån som klustret av punkter förskjuts uppåt eller neråt, då x-värdet stiger, demonstrerar dessa grafer ett samband mellan den ifrågavarande oberoende variabeln och sannolikheten för att den binära beroende variabeln skall få värdet 1.

De grafer som har en punkt per x-värde visar förhållandet mellan variabeln på x-axeln och medelvärdet (eng: *Mean*) för den predicerade sannolikheten för att den binära beroende variabeln skall få värdet 1. Det föregående avsnittets regressionsanalys visade vilket sambandet var mellan de oberoende variabelnas värden och de loggade oddsen för den beroende variabeln. Dessa grafer visar alltså istället sannolikhetsvärden och kan därför vara något lättare att tyda. I följande två grafer syns förhållandet mellan graden av institutionellt förtroende och sannolikheten för att vara orolig i förhållande till övervakning online. Som exempel:

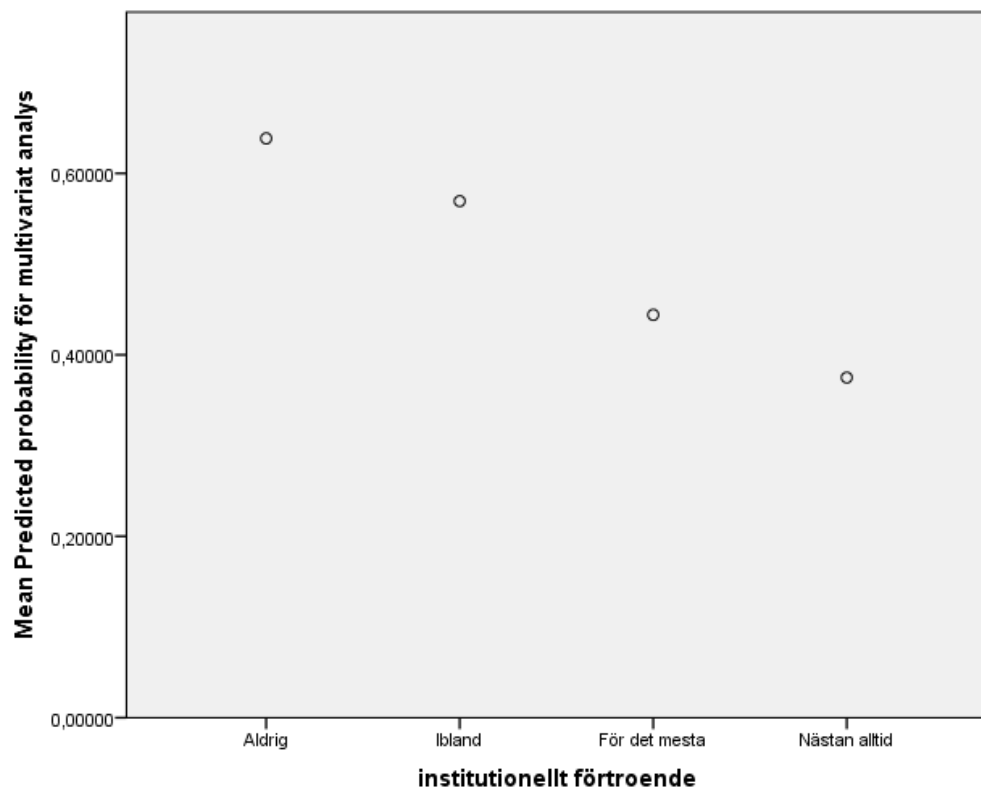
Ett värde på 0,65 på y-axeln, som är ungefär det värde personer som ansett att de aldrig litar på myndigheterna i genomsnitt har, innebär att en person med denna nivå av institutionellt förtroende med kring 65 % sannolikhet, anser att hen är orolig i förhållande till statens övervakning via internet, medan motsvarande siffra för personer som nästan alltid anser att myndigheterna går att lita på är kring 40 %.

Följande par av grafer visar förhållandet mellan kännedom om statlig övervakning med syfte att motverka terrorism och motsvarande sannolikhetsvärden. Dessa fyra första grafer demonstrerar alltså grafiskt det samband som regressionsanalyserna gav till känna.

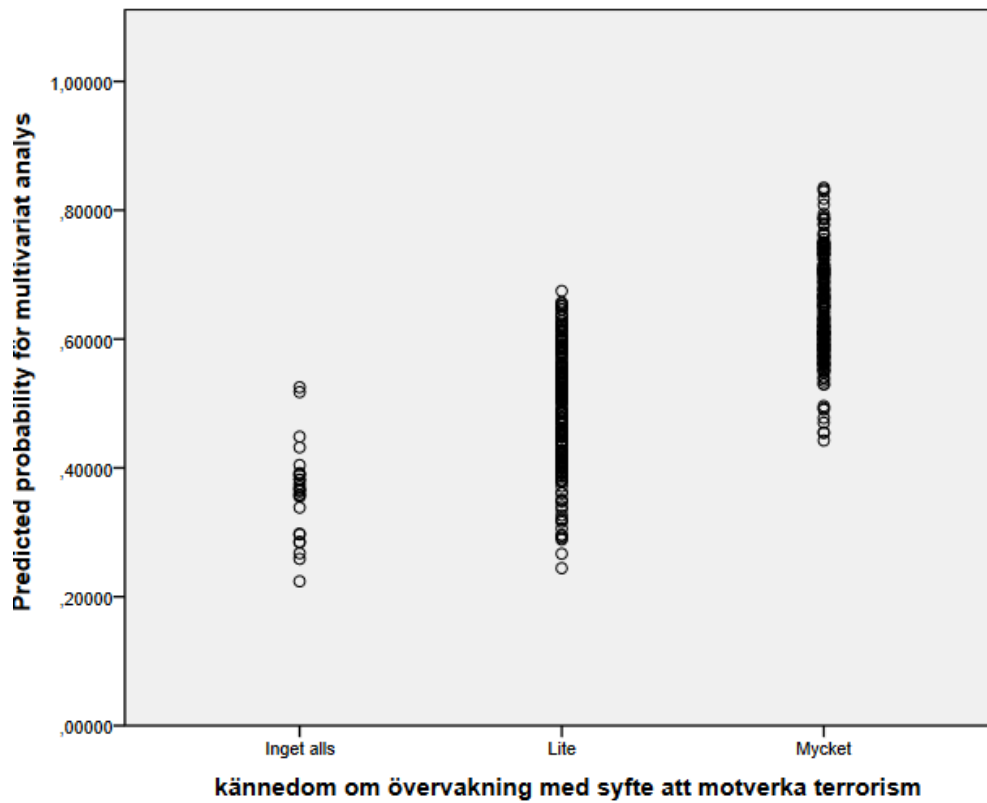
Graf 1: Sannolikhetsvärden för olika utfall för institutionellt förtroende



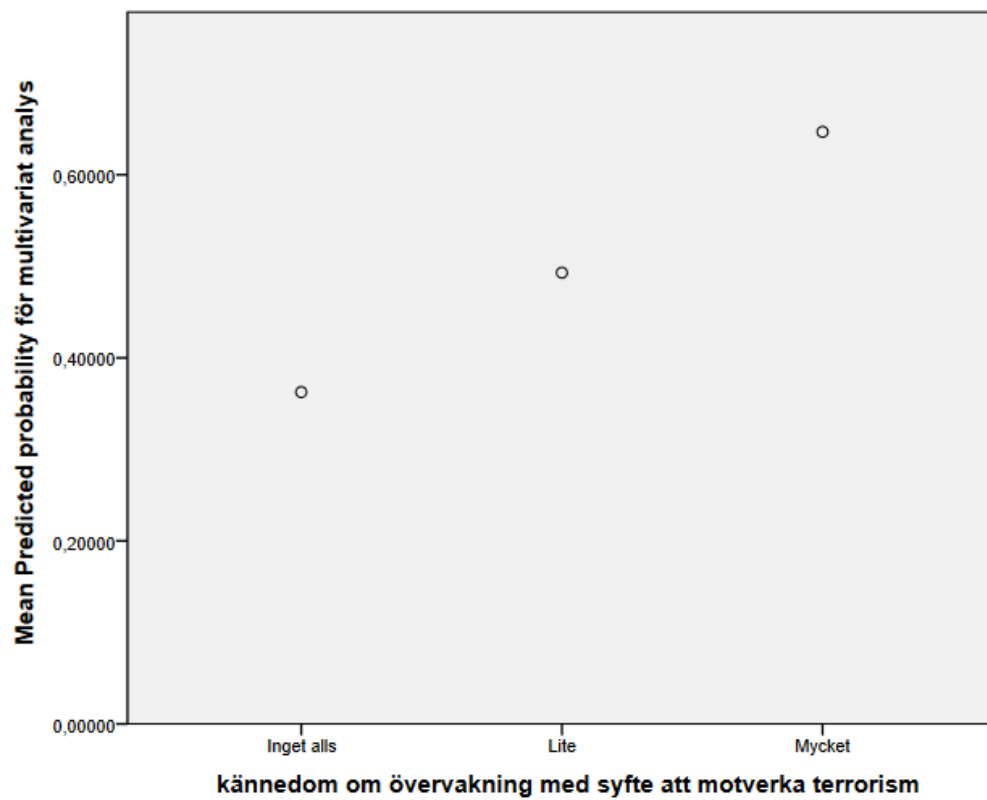
Graf 2: Sannolikhetsvärden för olika utfall för institutionellt förtroende, genomsnitt



Graf 3: Sannolikhetsvärden för olika utfall för kännedom om statlig övervakning med syfte att motverka terrorism

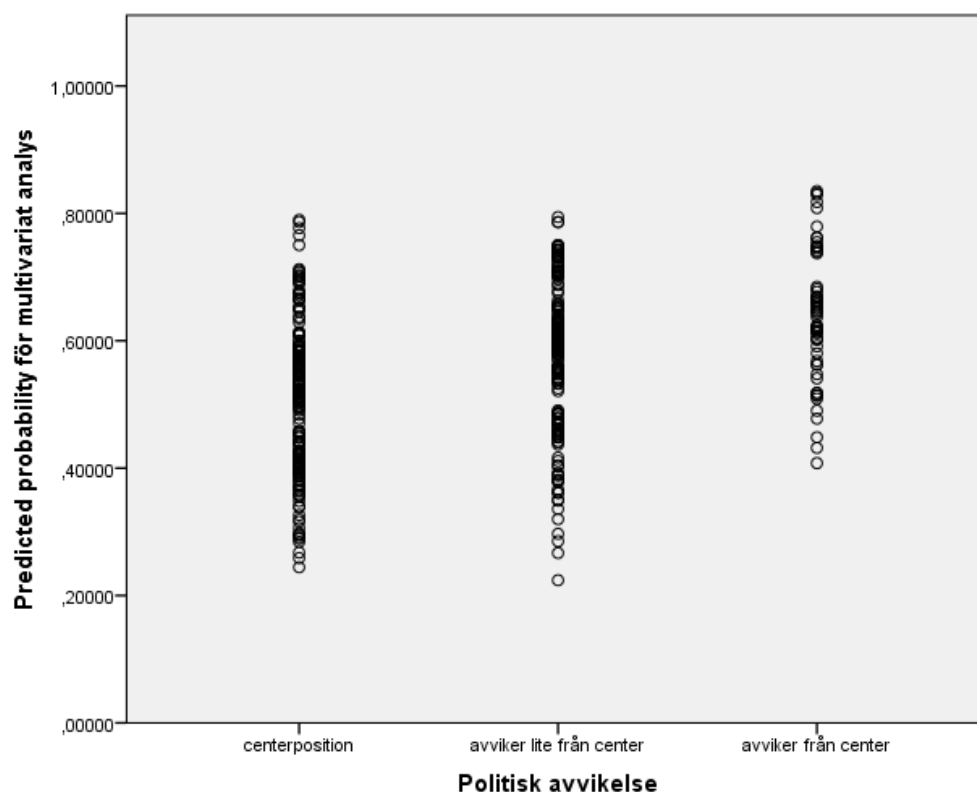


Graf 4: Sannolikhetsvärden för olika utfall för kännedom om statlig övervakning med syfte att motverka terrorism

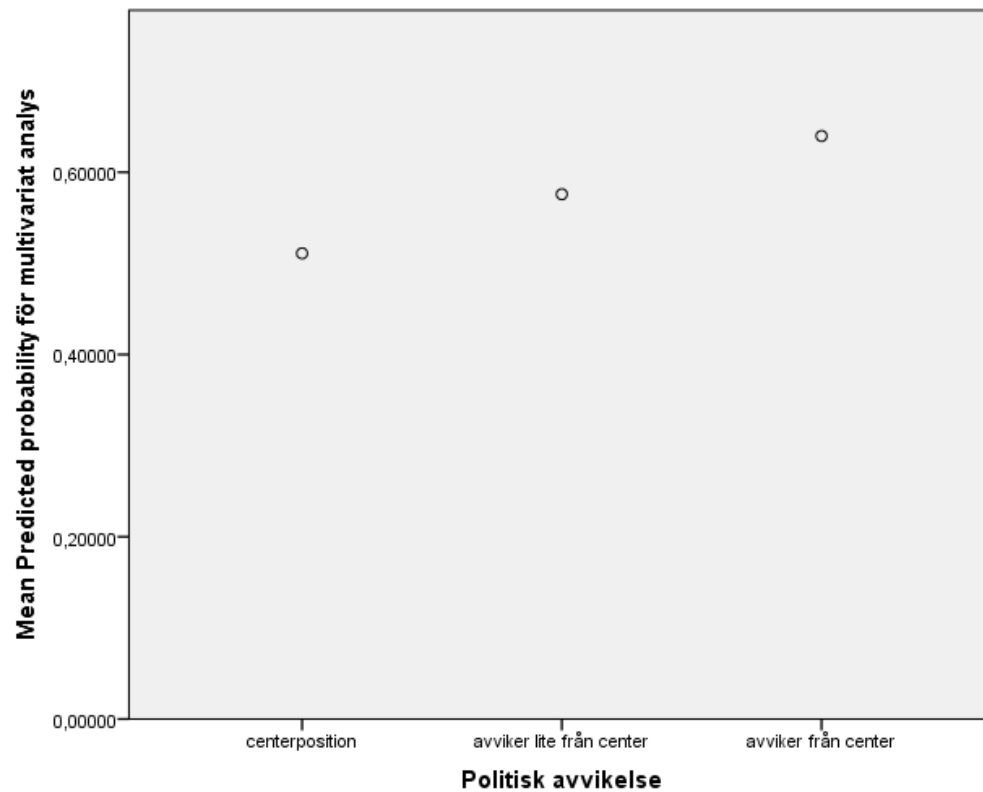


Följande fyra grafer visar förhållandet mellan politisk avvikelse och sannolikhetsvärden för att den binära beroende har ett värde 1. I de logistiska regressionsanalyserna var sambandet inte signifikant men som grafen visar finns det skillnader mellan de olika grupperna, framförallt då man ser på människors placering på en politisk höger-vänster skala och sannolikheten att anse sig vara orolig till statlig övervakning online. Genomsnittsvärdet för dem som klart avviker från den politiska centern i sin positionering, är kring 15 procentenheter högre än för dem som positionerar sig själva inom den politiska centern. Dock kan denna gradvisa förändring inte anses vara helt tillförlitlig, då resultatet inte är statistiskt signifikant.

Graf 5: Sannolikhetsvärden för olika utfall för politisk avvikelse

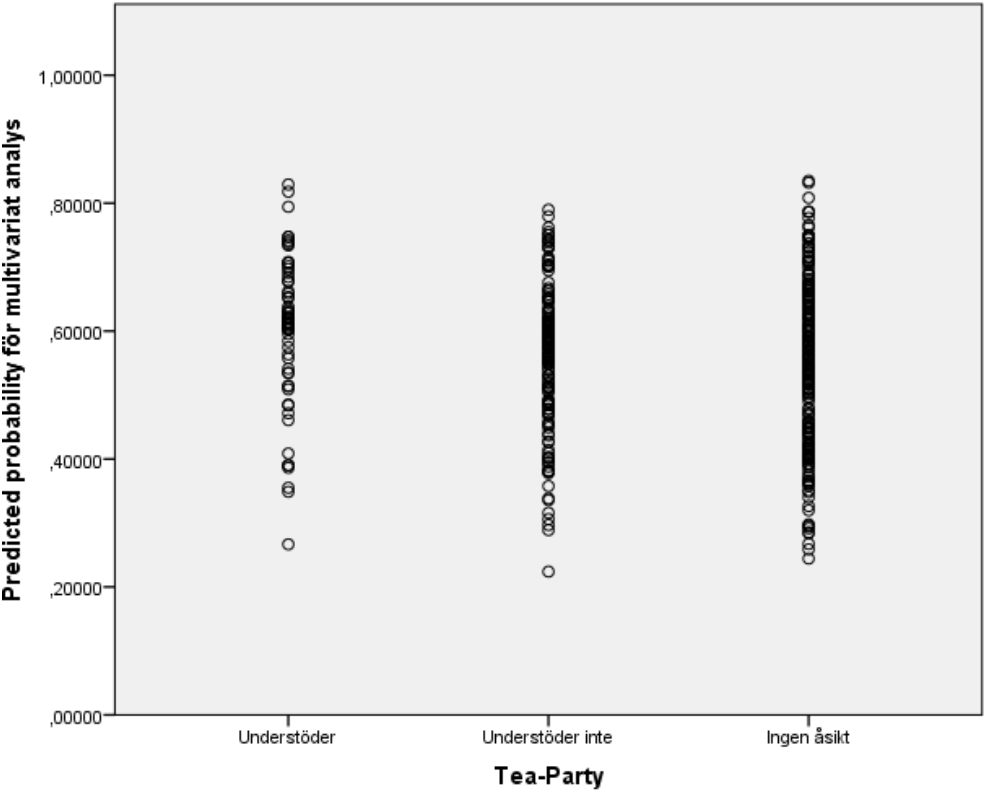


Graf 6: Sannolikhetsvärden för olika utfall för politisk avvikelse, genomsnitt

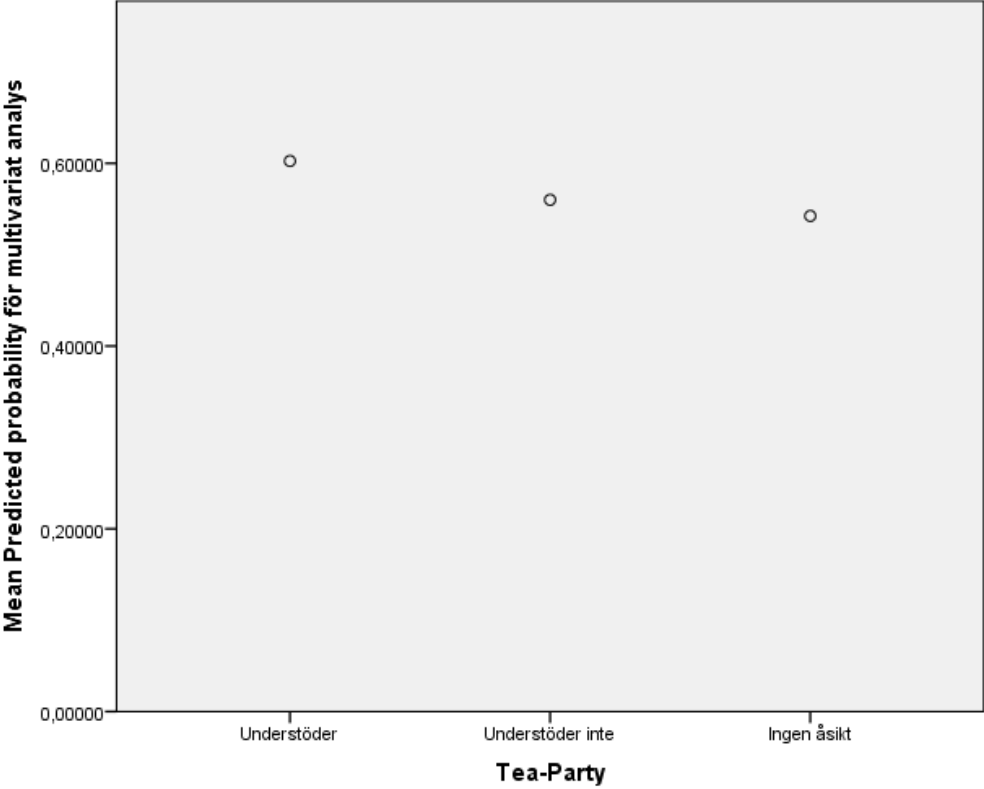


Då man ser på understöd för Tea party rörelsen kan resultatet vid en första anblick verka tyda på en klar skillnad mellan de som understöder och de som inte understöder. Denna uppfattning korrigeras av en uträkning av medelvärden, som visar på en väldigt liten skillnad. I de logistiska regressionsanalyserna var resultatet dessutom inte heller signifikant.

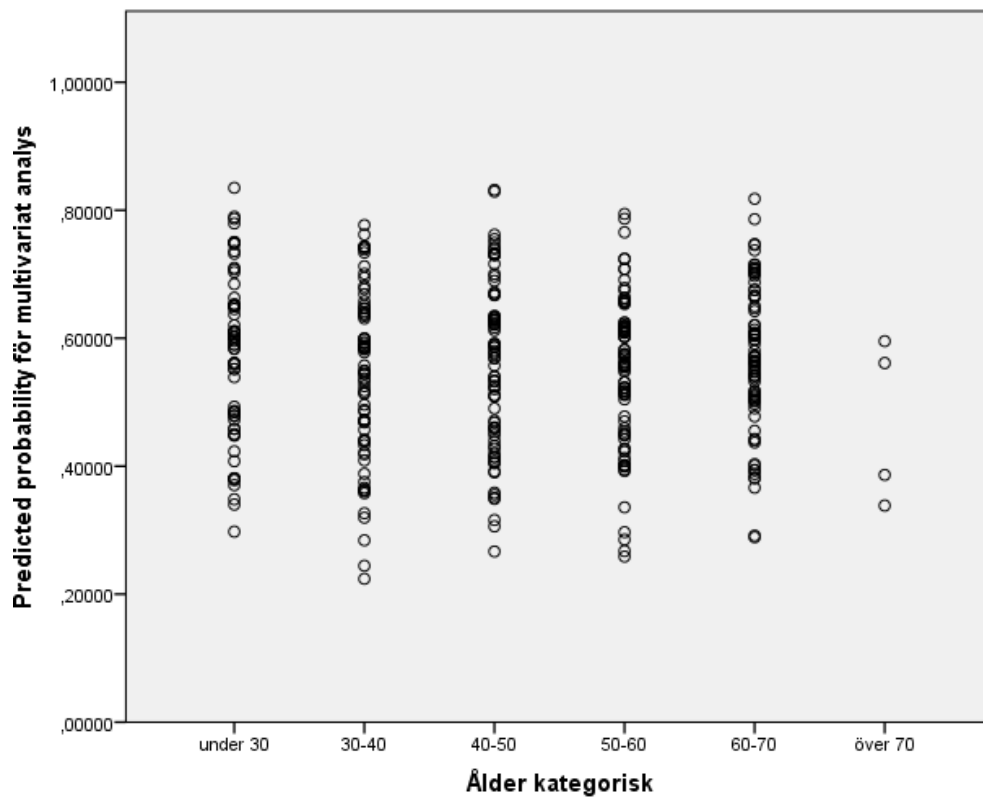
Graf 7: Sannolikhetsvärden för olika utfall för Tea Party understöd



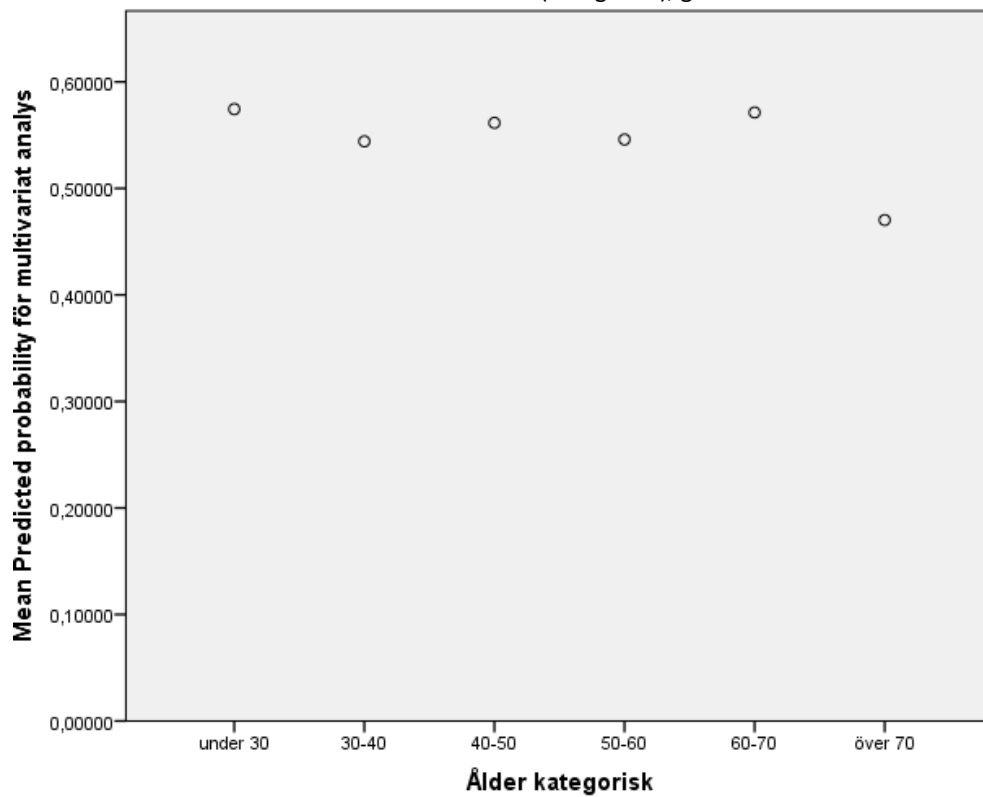
Graf 8: Sannolikhetsvärden för olika utfall för Tea Party understöd, genomsnitt



Graf 9: Sannolikhetsvärden för olika utfall för ålder (kategorisk)



Graf 10: Sannolikhetsvärden för olika utfall för ålder (kategorisk), genomsnitt



Graferna för ålder och sannolikhetsvärden för den binära beroende variabeln visar inget speciellt tydligt mönster gällande sambandet mellan ålder och attityd till integritet

online. Det enda värde som klart avviker, är för personer över 70, men denna kategori består av enbart 5 personer, så en sådan avvikelse är närmast intetsägende.

## 6. Diskussion och konklusion

Efter att i det föregående kapitlet ha gått igenom resultatet av min statistiska analys, kommer jag i detta kapitel att koppla detta resultat till de hypoteser jag formulerade på sidan 27. Om de kausala samband som hypoteserna föreslår gäller, innebär det att variablerna som hypotesernas begrepp är relaterade till måste ha ett statistiskt samband, så länge detta samband kan isoleras från externa faktorer med hjälp av kontrollvariabler. De samband mellan oberoende variabler och den beroende variabeln, som är i den riktning den relaterade hypotesen föreslår, ger alltså stöd åt denna hypotes. Om en oberoende variabel som, på basis av hypoteserna, borde ha ett statistiskt samband till den beroende variabeln, inte har det, innebär detta att hypotesen sannolikt är inkorrekt. Följande hypoteser testades i analysen:

**H1:** Ålder har ett negativt samband till en individs oro gällande myndigheters övervakning på internet.

**H2:** Högre förtroende för myndigheter har ett negativt samband till en individs oro gällande myndigheters övervakning på internet.

**H3:** Det finns ett positivt samband mellan hur politiskt avvikande någon är och denna individs oro gällande myndigheters övervakning på internet.

**H4:** Kännedom om statlig elektronisk övervakning med syfte att motverka terrorism har en negativ effekt på en individs oro gällande myndigheters övervakning på internet.

Att ålder har ett negativt samband till hur orolig någon är gällande myndigheters övervakning på internet, så som den första hypotesen påstår, fick inte stöd i den statistiska analysen. Resultatet visade visserligen ett negativt samband mellan ålder och den beroende variabeln, men eftersom signifikansvärdet var 0,65 kan analysen inte anses stöda hypotesen. Tidigare forskningsresultat från undersökningar gällande den brittiska befolkningen visar en koppling mellan attityder gällande integritet och ålder (Bakir m.fl. 2015). Man har funnit en negativ koppling mellan ålder och hur oroliga människor är att deras rätt till privatliv blir kränkt. Trots att min analys visade ett



negativt samband mellan ålder och oro i förhållande till övervakning online, vilket inte skiljer sig väsentligt från “oro att ens rätt till privatliv blir kränkt”, kan min analys inte anses bekräfta dessa tidigare resultat med en tillräckligt hög nivå av tillförlitlighet. Även de äldsta respondenterna verkar alltså dela uppfattningen att den amerikanska statens övervakning online är något att känna oro inför. Denna ålderskategori har visat mera tolerans i tidigare undersökningar som gjorts, men i denna undersökning är dessa personer på samma linje som resten av befolkningen. Orsaken till att detta är fallet är inte klar, men en möjlig anledning skulle kunna tänkas vara att den fråga som jag använt för att mäta oro till övervakning online av staten även inkluderar telefonsamtal, då det som frågas om är “electronic communication”. Äldre personer är möjligtvis inte lika oroliga i förhållande till sådan datainsamling som sker om t.ex. webbläsarhistorik eller email, då de inte är lika aktiva användare av sådana tjänster (Clement, 2019). När frågan även handlar om sådant de är aktiva användare av, kan det eventuellt producera ett annorlunda resultat. Detta skulle innebära en viss validitetsbrist i det mått jag använt mig av.

Vad det gäller institutionellt förtroende visade den statistiska analysen ett signifikant negativt samband till den beroende variabeln. Jag fann alltså stöd för den andra hypotesen. Tidigare undersökningar som gjorts föreslår att det finns ett positivt samband mellan hur stort någon anser att behovet av övervakning är och deras institutionella förtroende (Massimo m.fl., 2005). En möjlig förklaring till att personer som har ett högre institutionellt förtroende, har en lägre nivå av oro i förhållande till övervakning online av myndigheterna, skulle kunna tänkas vara att de ser sådan övervakning som mera nödvändig och därför inte fäster lika mycket uppmärksamhet vid dess potentiella negativa sidor.

Tidigare forskningsresultat visar även ett negativt samband mellan hur stort någon anser att behovet av övervakning är och hur oroliga de är att sådan information de delar vid ekonomiska transaktioner på nätet, används på ett olämpligt sätt (Dinev m.fl., 2008) . Om detta samband även gäller det ansedda behovet av övervakning och oro i förhållande till myndigheternas insamlande av information, kan det förklara hur institutionellt förtroende är relaterat till attityder till integritet online. Institutionellt förtroende kan kanske tänkas få människor att anse att det finns ett större behov av övervakning, alltså att övervakning är en lösning på vissa problem, vilket får dem att

fokusera mindre vid potentiella negativa sidor och därmed vara mindre oroliga. Förtroende kan alltså även handla om statens kompetens för problemlösning.

Alternativt är förklaringen den jag baserade min hypotes på d.v.s. att människor som har mindre förtroende för myndigheterna anser att risken är högre att den information myndigheterna samlar in används på ett sätt som skadar dem. Då staten hävdar att den utför sådan informationsinsamling med amerikanska invånares intresse i åtanke, kommer personer med lägre institutionellt förtroende alltså att tendera att vara mera skeptiska till att detta stämmer. Det gör dem i sin tur mindre villiga att understöda sådan informationsinsamling. Det handlar alltså om en direkt inverkan av institutionellt förtroende på människors attityd till integritet. En kombination av dessa två mekanismer skulle förstås även kunna vara gällande. I hur hög utsträckning människor anser att myndigheterna går att lita på, visade i vilket fall som helst ha ett samband till deras nivå av oro gällande statlig övervakning online. Då man frågar sig vad som är avgörande för människors attityd till integritet på internet, verkar deras nivå av institutionellt förtroende utgöra en del av svaret. Det kanske inte är så överraskande att förtroende för en av de aktörer som samlar in personlig information om en som person, påverkar ens attityd till sådan informationsinsamling.

För att testa den tredje hypotesen gällande politisk avvikelse använde jag mig av den oberoende variabeln "Politisk avvikelse" men analyserade även sambandet mellan den beroende variabeln och understöd för Tea party rörelsen. För att hypotesen skall stämma borde personer som har ett högre värde för "Politisk avvikelse" och därmed placerar sig längre från den politiska centern, generellt sätt uttrycka större oro i förhållande till myndigheters övervakning online. Jag förväntade mig därutöver att personer som understöder Tea party rörelsen i allmänhet skulle uttrycka större oro. Analysen visar ett positivt samband för båda dessa variabler, men resultatet nådde inte statistisk signifikans. Det innebär tyvärr att jag inte kan avgöra huruvida dessa två variabler verkligen påverkar variationen i den beroende variabeln eller inte. Huruvida politisk avvikelse har en positiv effekt på hur oroliga människor är i förhållande till statlig övervakning online förblir en öppen fråga.

Den fjärde och sista hypotesen som testades fick inte stöd i den statistiska analysen. Kännedom om statlig övervakning med syfte att motverka terrorism hade ett signifikant positivt samband till oro gällande myndigheters övervakning online. Resultatet var med

andra ord det rakt motsatta till vad jag förväntade mig. Tidigare forskning visar hur människor är mera toleranta till statlig övervakning efter terroristattentat. Givet att analysens resultat är tillförlitligt, verkar det som om myndigheternas försök att motivera övervakning med hotet av flera attentat inte har haft en liknande effekt på allmän opinion. Det är dock värt att komma ihåg att denna undersökning gjordes efter att Edward Snowden hade avslöjat vissa potentiella missbruk av övervakningskompetens av de amerikanska myndigheterna. De som hade hört mycket om hur myndigheterna övervakar med syfte att trygga nationell säkerhet, hade även troligen hört en hel del om de negativa sidorna hos denna övervakning.

Vad kan man därmed säga om debatten om behovet av övervakning för mera säkerhet v.s. skyddande av människors rätt till privatliv, givet det positiva sambandet mellan “kännedom om statlig övervakning med syfte att motverka terrorism” och “oro gällande övervakning online? Det verkar som om de personer som följt med sådan övervakning även sannolikt varit mera medvetna om denna debatt. Om man antar att det finns ett kausalt samband mellan dessa variabler, snarare än ett skensamband, verkar en möjlig förklaring vara att personer som är mera medvetna om denna statliga aktivitet, har blivit allt mera kritiska till dess legitimitet, desto mera de hört om denna. I den mån som debatten om säkerhet och integritet varit en del av den information de blivit medvetna om, kan argumenten gällande behovet av integritetsskydd i förhållande till statsmakten antas ha varit mera övertygande, därmed känner de sig mera oroliga. Till någon mån kan detta understöda påståendet, att de som understöder mera skydd för privatliv varit vinnare i denna debatt, enligt den amerikanska allmänheten. Dock är förstås ställningstagande inom debatten om säkerhet v.s. integritet inte synonyma med graden av oro gällande övervakning och därmed krävs det att man gör sådana slutsatser försiktigt, då det finns andra möjliga förklaringar.

Då man frågar sig vilken information som människor mera specifikt kommit i kontakt med då de följt med detta ämne, är förstås Edward Snowdens information om de amerikanska myndigheterna av central betydelse. Det verkar sannolikt då de enkätundersökningar som denna analys grundar sig utfördes direkt efter att denna information blev allmänt känd med det uttalade syftet att avgöra effekten av denna incident på allmän opinion. Då man studerat motsvarande effekt inom den brittiska befolkningen, fann man att hela 60 % procent ansåg sig vara mera oroliga än för ett år sedan, då de frågades efter att Snowdens information kommit till allmän kännedom

(Bakir m.fl. 2015, 8). Att finna ett positivt samband mellan kännedom om statlig övervakning med syfte att motverka terrorism och nivån av oro i förhållande till myndigheters övervakning online kan kanske finna en förklaring inom den situation som rådde under de kommande åren efter denna händelse.

För att återgå till den fråga vars svar fungerar som ett mått för variabeln "kännedom om statlig övervakning med syfte att motverka terrorism": How much, if anything, have you heard about the government collecting information about telephone calls, emails and other online communications as part of efforts to monitor terrorist activity?. De som hört mera har trots motiveringen, att övervaka terroristaktivitet, inte blivit övertygade om denna övervaknings nödvändighet utan uttrycker i stället mera oro. Det är förstås möjligt att de som hade hört mycket om övervakning med syfte att motverka terrorism, hade en annan attityd innan Snowdens publikation och att sambandet mellan variablerna såg rätt så annorlunda ut vid en tidigare tidpunkt. Det går dock utanför gränserna för denna undersökning. Teoretiskt sätt kan det i alla fall tänkas ge en möjlig förklaring till dessa variablers samband. Det är dock viktigt att inte överskatta betydelsen av sådana enskilda händelser. I fallet av Storbritannien har trenden exempelvis varit en uppgång av oro i förhållande till statlig övervakning, även före Snowden. Dessutom var denna studie (Bakir m.fl. 2015, 8) inte en studie på individnivå, vilket innebär att de samband man ser på landnivå kan vara frånvarande då man undersöker enskilda människor, såsom inom den analys jag har gjort.

En fråga gällande detta samband är alltså huruvida de personer som av en eller annan anledning hört mera om statlig övervakning online med syfte att motverka terrorism, redan på förhand var mera oroliga eller om deras större oro var en konsekvens av att de blev mera medvetna om ämnet. En person kan förstås vara principiellt emot statlig övervakning och därför känna större oro vilket får denna person att söka upp information om ämnet. Det skulle innebära att den kausala relationen följer det omvända mönstret till vad jag antagit. Trots att den oberoende variabeln har mätts före den beroende, verkar det som om denna möjlighet kvarstår. De utmaningar som hör ihop med att etablera kausala samband på basis av statistisk analys diskuterades tidigare i kapitel 7, under rubriken: kausalitet. Vad det gäller hur olika variabler påverkar varandra är det förstås frågan om statistiska samband och inte nödvändigtvis en direkt kausal effekt, så som även diskuterades tidigare i kapitel 7. De statistiska samband som analysen visar gör dock eventuella kausala samband mera sannolika.

Institutionellt förtroende och hur mycket människor har hört om statens övervakning med syftet att motverka terrorism, har båda ett samband med deras attityd till integritet i termer av hur oroliga de är i förhållande till statlig informationsinsamling gällande elektronisk kommunikation. Personer som har lägre förtroende för staten och har hört mera om sådan informationsinsamling upplever mera oro. Detta kan naturligtvis handla om huruvida det man som amerikansk medborgare, under åren före denna undersökning, hörde om statens informationsinsamling t.ex. i samband med Edward Snowdens informationsläcka. När det gäller "Kännedom om statlig elektronisk övervakning med syfte att motverka terrorism" kan det med andra ord vara svårt att generalisera detta resultat.

Hade det som fanns att höra om sådan övervakning varit mera positivt i förhållande till den amerikanska statens övervakning, kunde att höra mera om sådan aktivitet eventuellt haft motsatt eller neutral inverkan. Om Snowden aldrig publicerat den information han *de facto* publicerade hade den allmänna opinionen kunnat se något annorlunda ut. Detta samband framstår alltså som högst beroende av det aktuella läget i USA vid tidpunkten för undersökningen. Att institutionellt förtroende samvarierar med människors attityd till online-integritet kan, också med stöd av tidigare forskningsresultat, generaliseras med större tillförlitlighet. På basis av min analys blir det därmed svårt att ge ett generellt svar på vad som förklarar människors attityd till integritet online.

De som har lägre institutionellt förtroende är mera oroliga gällande statlig övervakning, vilket förklarar en del av den attityd de har till integritet på internet i förhållande till myndigheterna. I vilken mån olika argument som framförts i den offentliga debatten påverkat allmän opinion är svårt att avgöra, dock har de amerikaner som sannolikt hört mera om denna debatt och rapportering om den amerikanska statens övervakning under mitten av 2010-talet, blivit mera oroliga. Trots att innehållet i den information dessa personer hört om statlig övervakning inte är en del av denna analys, kan det i alla fall konstateras att den offentliga debatten och medierapportering om detta ämne inte verkar ha varit verkningslös. Ytterligare forskning skulle eventuellt kunna visa vilka delar av denna information som den amerikanska befolkningen kommit i kontakt med, som varit avgörande för deras ökade oro.

## 7. Avslutning

Bakgrunden till människors attityder till övervakning och integritet hör ihop med ett viktigt vägval som samhället står inför. I och med att internets tidsålder har inletts, måste vi potentiellt omdefiniera förhållandet mellan stat och individ beträffande integritet. Den kapacitet för övervakning som finns i dagens samhälle skapar ett val mellan vissa individuella rättigheter, såsom rätten till privatliv, och upprätthållandet av nationell säkerhet, brottsbekämpning samt olika kommersiella fördelar. Då människors attityd avgörs i denna fråga är det möjligt att de väger tänkta för- och nackdelar mot varandra och kommer till en slutsats om hur dessa värden skall balanseras. Huruvida människors attityder avgörs genom rationella överväganden eller på basis av andra mekanismer får förbli osagt. Dock är mitt intryck av samhällsdebatten att många upplever sig obekväma med tanken på att vara övervakade. Människor kan inte alltid säga varför de uppskattar skydd av privatliv, men de enkätundersökningar som gjorts visar att allmänheten ser det som viktigt och är oroliga över att förlora det.

En faktor som naturligtvis styr hurudan inställning människor har till statlig övervakning, är deras uppfattning av vad det är som staten mera specifikt gör. I vilken mån den amerikanska allmänheten känner till detta eller vad deras uppfattning är om hur de amerikanska myndigheterna bedriver övervakning online har inte inkluderats i denna analys. Det skulle ha krävt ytterligare data. Dock verkar det sannolikt att de personer som har hört mera om övervakning online med syftet att motverka terrorism även vet mera om ämnet. Då dessa personer hört vad staten gjort, har de på basis av denna information kunnat bilda sig en egen uppfattning om huruvida detta varit rätt eller fel, samtidigt som de kommit i kontakt med de olika argument som kritiker och försvarare av denna övervakning framfört.

Det är viktigt att hålla i tankarna att de argument som kritiker mot de amerikanska myndigheternas övervakning framför, först och främst är kritik gällande massövervakning, snarare än kategoriska argument gällande statlig övervakning. Mycket av argumentationen efter incidenten med Edward Snowden har kretsat kring huruvida NSA borde få samla in information om den stora allmänheten, d.v.s. utföra massövervakning. Även de största kritikerna till statlig övervakning tenderar att hålla med om, att statens uppgift som upprätthållare av säkerhet och ordning inte är möjlig

utan övervakning. Att använda de elektroniska resurser som finns tillgängliga är, i dagens internetanvändande värld, närmast självklart. Frågan är i stället om massövervakning är berättigat. Det verkar realistiskt att tänka sig att människor med tiden blir mindre obekväma med att myndigheter, samt stora IT-företag, känner till allt mera om deras liv. Ett samhälle där människors integritet är svagare än vad som varit fallet traditionellt sätt verkar sannolikt. Dock ser det ut som om den allmänna opinionen är emot massövervakning.

Då man försöker avgöra var man står i denna fråga är huruvida man litar på myndigheterna en av de saker man sannolikt grundar sin bedömning på. Kommer staten att använda sin kompetens på ett etiskt sätt eller inte? Sist och slutligen är det inte enbart en fråga om huruvida man litar på den stat som för tillfället existerar, utan en mera generell fråga. Om vi väljer att ge staten större övervakningskompetens i dagens samhälle, är det långsiktigt hållbart? Då vilka politiska grupper som i praktiken har makten varierar över tid, kan man fråga sig om det system vi skapar kommer att undvika felanvändning av denna maktbefogenhet på lång sikt av de som har kontroll över staten. De institutionella vägval som görs i dagens samhälle kan få långtgående konsekvenser för framtidens samhällsutveckling. Det finns både historiska och samtida exempel på hur övervakning kan användas för att upprätthålla förtryck och större övervakningskapacitet stärker auktoritära regimers förmåga till detta. Om regimen inte missbrukar sin makt kan dock övervakningskompetens användas för det allmänna bästa. Vad som är mera sannolikt blir en fråga om institutionellt förtroende och i vilken mån makt korrumpierar.

.

## 8. Källor:

- Acquisti, Alessandro. (2004). *Economics of Information Security*. s. 184-185  
[https://link.springer.com/content/pdf/10.1007/1-4020-8090-5\\_14.pdf](https://link.springer.com/content/pdf/10.1007/1-4020-8090-5_14.pdf)
- Bakir, Vian. Cable, Jonathan. Dencik, Lina. Hintz, Arne. McStay, Andrew. (2015).  
*Public Feeling on Privacy, Security and Surveillance*. A Report by DATA-PSST and DCSS.
- Bennett, Colin J. (1995) *Privacy in the Political System: Perspectives from Political Science and Economics*. A report written for the Ethical, Legal and Social Issues (ELSI) component of the Human Genome Project, U.S. Department of Energy (1995, revised 2001).
- Bjerling, Johannes & Ohlsson Jonas. 2010. *En introduktion till logistisk regressionsanalys*. Göteborg: Göteborgs Universitet Arbetsrapport nr 62.  
[https://jmg.gu.se/digitalAssets/1307/1307026\\_Nr\\_62\\_Logistisk\\_regression.pdf](https://jmg.gu.se/digitalAssets/1307/1307026_Nr_62_Logistisk_regression.pdf)
- Clement, J. (2019). *U.S. adult internet usage reach 2000-2018, by age group*. New York: Statista, inc. <https://www.statista.com/statistics/184389/adult-internet-users-in-the-us-by-age-since-2000/>
- Dinev, Tamara. Hart, Paul. Mullen, Michael R. (2008). *Internet privacy concerns and beliefs about government surveillance – An empirical investigation*. Journal of Strategic Information Systems 17, s. 214–233.
- Esaiasson, Peter. Gilljam, Mikael. Oscarsson, Henrik. Wägnerud, Lena. (2012).  
*Metodpraktikan: konsten att studera samhälle, individ och marknad*. Stockholm: Norstedts juridik.
- Evans, Jennifer. (2002). *Hijacking Civil Liberties: The USA PATRIOT Act of 2001 Comment*. Chicago: Loyola University Chicago Law Journal 33. Issue 4 - Summer 2002 s. 933.  
[https://heinonline.org/HOL/Page?handle=hein.journals/luclj33&div=41&g\\_sent=1&casa\\_token=&collection=journals](https://heinonline.org/HOL/Page?handle=hein.journals/luclj33&div=41&g_sent=1&casa_token=&collection=journals)
- Holvast Jan. (2009). *History of Privacy*. Landsmeer: Holvast & Partner.



- Kannan P. K. Rust, Roland T. Peng, Na. (2002). *The Customer Economics of Internet Privacy*. Journal of the Academy of Marketing Science-October 2002.
- Landman, Todd. (2003). *Issues in and Methods An Comparative Introduction Politics*. New York: Routledge
- Li, Yaoi. Kobsa, Alfred. Knijnenburg, Bart P. Nguyen, Carolyn . *Cross-Cultural Privacy Prediction*. s.123-124. Proceedings on Privacy Enhancing Technologies ; 2017 (2):113–132. <https://petsymposium.org/2017/papers/issue2/paper28-2017-2-source.pdf>. DOI 10.1515/popets-2017-0019.
- Massimo, Bellotto. Dinev, Tamara. Hart, Paul. Colautti, Christian. Vincenzo, Russo. (2005). *Internet Users, Privacy Concerns and Attitudes towards Government Surveillance - An Exploratory Study of Cross-Cultural Differences between Italy and the United States*. BLED 2005 Proceedings. 30.
- Movius, Lauren B. Krup, Nathalie. (2009). *U.S. and EU Privacy Policy: Comparison of Regulatory Approaches*. International Journal of Communication 3 (2009), s. 169-187.
- Papacharissi, Zizi A. (2010). *A private sphere, democracy in a digital age*. Cambridge: Polity Press.
- Patil, S. Patruni, B. Hui, L. Dunkerley, F. Fox, J. Potoglou, D. Robinson, N. (2015). *Public perception of security and privacy*. Santa Monica, Calif., and Cambridge, UK: RAND Corporations.
- Pew Research Center. *Privacy Panel #1*. [dataset], Washington: Pew Research Center, 2014. <https://www.pewresearch.org/internet/dataset/january-2014-privacy-panel-1/> . hämtad 10 januari 2019.
- Pew Research Center. *Privacy Panel #3*. [dataset], Washington: Pew Research Center, 2015. <https://www.pewresearch.org/internet/dataset/november-2014-privacy-panel-3/>. hämtad 10 januari 2019.
- Potoglou, Dimitris. Dunkerley, Fay. Patil, Sunsil. Robinson, Neil. (2017). *Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study*. Computers in human behavior 75 s. 811-825.

- Rayport, Jeffrey F. & Hagel, John. (1997). *The Coming Battle for Customer Information*. Harvard Business Review (January–February 1997 Issue).  
<https://hbr.org/1997/01/the-coming-battle-for-customer-information>.
- Roser, Max. Ritchie, Hannah. Ortiz-Ospina, Esteban. (2019). *Internet*. Published online at OurWorldInData.org. Taget från: '<https://ourworldindata.org/internet>'  
[Online Resource]
- Rule, James B. (2009). *Privacy in Peril : How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience*. Oxford University Press USA - OSO(Oxford Scholarship Online).
- Schoeman, Ferdinand D. (1992). *Privacy and social freedom*. Cambridge: Cambridge University Press
- Solovet, Daniel J. (2003). *The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure* Solove, s. 993- 996. Durham: Duke Law Journal vol. 53 Issue 3 - December 2003.  
[https://heinonline.org/HOL/Page?handle=hein.journals/dukclr53&div=32&g\\_sent=1&asa\\_token=&collection=journals](https://heinonline.org/HOL/Page?handle=hein.journals/dukclr53&div=32&g_sent=1&asa_token=&collection=journals)
- Stratford, Jean S. & Stratford, Juri. (1998). *Data Protection and Privacy in the United States and Europe*. IASSIST Quarterly.
- Trepte, Sabine. Reinecke, Leonard. Ellison, Nicole B. Quiring, Oliver. Yao, Mike Z. Ziegele, Marc. (2017). *A Cross-Cultural Perspective on the Privacy Calculus*. SAGE journals, Volume: 3, Issue: 1. issue:<https://journals.sagepub.com/doi/full/10.1177/2056305116688035>
- Westin, Alan .F. (2003). *Social and Political Dimensions of Privacy*. Journal of Social Issues, Vol. 59, No 2.
- Whitten, Guy D. & Kellstedt, Paul M. (2013). *The Fundamentals of Political Science Research*. New York: Cambridge University Press.
- Zavrsnik, Ales. & Levicnik, Pia. (2015). *The public perception of cyber-surveillance before and after Edward Snowden's surveillance revelations*. Masaryk University Journal of Law and Technology.

## 9. Bilagor:

Ordinal logistisk regressions analys output:

Parameter Estimates						
		Estimate	Std. Error	Wald	df	Sig.
Threshold	[beroende_var = 1,00]	-1,222	,571	4,575	1	,032
	[beroende_var = 2,00]	,667	,566	1,390	1	,238
	[beroende_var = 3,00]	2,640	,580	20,713	1	,000
Location	ålder	-,003	,006	,206	1	,650
	pol_avv	,177	,134	1,739	1	,187
	inst.förtroende	-,387	,154	6,265	1	,012
	Utbild	,107	,093	1,337	1	,248
	känn_anti_terr_overv	,639	,162	15,475	1	,000
	[kön=1,00]	-,298	,186	2,574	1	,109
	[kön=2,00]	0 <sup>a</sup>	.	.	0	.
	[Tea_Party_1=1,00]	,537	,284	3,573	1	,059
	[Tea_Party_1=2,00]	-,120	,207	,336	1	,562
	[Tea_Party_1=3,00]	0 <sup>a</sup>	.	.	0	.

Tabell 16 Resultat av multivariat analys med ordinal beroende variabel

Parameter Estimates			
		95% Confidence Interval	
		Lower Bound	Upper Bound
Threshold	[beroende_var = 1,00]	-2,342	-,102
	[beroende_var = 2,00]	-,442	1,776
	[beroende_var = 3,00]	1,503	3,777
Location	ålder	-,013	,008
	pol_avv	-,086	,440
	inst.förtroende	-,689	-,084
	Utbild	-,075	,290
	känn_anti_terr_overv	,321	,958
	[kön=1,00]	-,663	,066
	[kön=2,00]	.	.
	[Tea_Party_1=1,00]	-,020	1,094
	[Tea_Party_1=2,00]	-,526	,286
	[Tea_Party_1=3,00]	.	.

Tabell 17 Resultat av multivariat analys med ordinal beroende variabel

